STMicroelectronics

MIFARE Plus® EV2 on ST31N600 A01
Security Target for composition

Common Criteria for IT security evaluation

SMD_MFPEV2_ST31N600_ST_22_002 Rev 01.1

March 2024

life.augmented

BLANK

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: MIFARE Plus EV2 on ST31N600 A01 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev 01.1, issued in March 2024.

3 Registration: registered at ST Microelectronics under number SMD_MFPEV2_ST31N600_ST_22_002.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the technology library **MIFARE Plus® EV2**[a] on the Security IC **ST31N600 A01.**

5 This TOE is a composite TOE, built up with the combination of:

- The Security IC **ST31N600 A01**, designed by STMicroelectronics, and used as certified platform,
- The technology library **MIFARE Plus EV2**, developed by STMicroelectronics, and built to operate with this Security IC platform.

6 Therefore, this Security Target is built on the Security IC Security Target *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*, referenced *BSI-CC-PP-0084-2014*.
The Security IC Security Target is called “Platform Security Target” in the following.

7 The precise reference of the Target of Evaluation (TOE) is given in *Section 1.4: TOE identification* and the TOE features are described in *Section 1.6: TOE description*.

8 A glossary of terms and abbreviations used in this document is given in *Appendix A: Glossary*.

[a] MIFARE and MIFARE Plus are registered trademarks of NXP B.V. and are used under license.

Contents

List of tables

List of figures

1.3 Context

9 The Target of Evaluation (TOE) referred to in *Section 1.4: TOE identification*, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Connected Security Division of STMicroelectronics (ST).

10 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by ALC_DVS.2, AVA_VAN.5 and ALC_FLR.1.

11 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE, and to summarise its chosen TSF services and assurance measures.
Since the TOE is a composite TOE, this Security Target is built on the Security IC Security Target *ST31N600 A01 Security Target for composition*, referenced *SMD_ST31N6000_ST_20_002*.

12 This ST claims to be an instantiation of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*" (PP) registered and certified under the reference *BSI-CC-PP-0084-2014* in the German IT Security Evaluation and Certification Scheme.

13 The Platform Security Target introduces the following augmentations:

- Addition #1: "Support of Cipher Schemes" from *[AUG]*
- Addition #4: "Area based Memory Access Control" from *[AUG]*.
- Additions specific to the Platform Security Target, some in compliance with *[JILSR]* and *ANSSI-PP0084.03*.

14 This Security Target introduces augmentations dedicated to MIFARE Plus EV2.

The original text of the PP is typeset as indicated here, its augmentations from *[AUG]* as indicated here, and text originating in *[JILSR]* as indicated here, when they are reproduced in this document.

15 This ST makes various refinements to the above mentioned PP and *[AUG]*. They are all properly identified in the text typeset as ***indicated here*** or ~~here~~. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: ***BSI*** for *BSI-CC-PP-0084-2014*, ***AUG1*** for Addition #1 of *[AUG]*, ***AUG4*** for Addition #4 of *[AUG]* and ***JIL*** for *[JILSR]*.

1.4 TOE identification

16 The Target of Evaluation (TOE) is the technology library MIFARE Plus EV2 on ST31N600 A01.

17 "MIFARE Plus EV2 on ST31N600 A01" completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 15: Guidance documentation*, and its development and production sites indicated in *Table 16: Sites list*.
Refer also to the corresponding tables in the *ST31N600 A01 Security Target for composition*.

Table 1. TOE components

Platform identification				Library identification
IC Maskset name	IC version	Master identification number	Firmware version	MIFARE Plus EV2 version
K470B	B	0x0200	3.1.2	1.0.2

18 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: TOE components*, and the configuration elements as detailed in the Data Sheet, referenced in the *ST31N600 A01 Security Target for composition*.

19 In this Security Target, the term "MFPEV2" means MIFARE Plus® EV2 1.0.2.

20 The MIFARE Plus EV2 User Manual, referenced in *Table 15: Guidance documentation,* details how to check the library integrity and version.

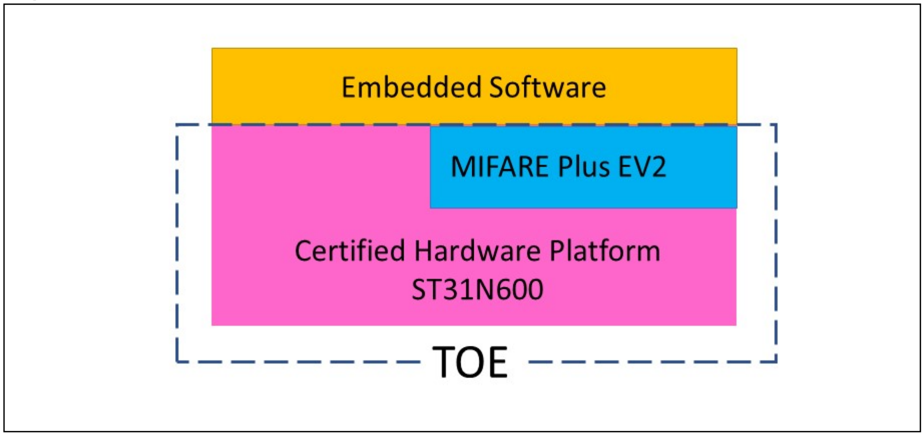
1.5 TOE overview

21 This TOE consists of a certified hardware platform and an applicative embedded software, MIFARE Plus EV2, stored in the hardware User NVM of the Platform.

22 The hardware platform is the ST31N600 with its firmware. It is identified as ST31N600 A01 which means it includes the components listed in the “Platform identification” columns in*Table 1: TOE components*, and detailed in the Security IC Security Target *ST31N600 A01 Security Target for composition*, referenced *SMD_ST31N6000_ST_20_002*.
The ST31N600 is designed to enable an effective usage of MIFARE Plus EV2, and underly its security functionality.
The Platform Security Target references the guidance documentation directly related to the hardware platform.

23 *Figure 1* provides an overview of the TOE.

Figure 1. TOE overview



24 The TOE is primarily designed for secure contact-less transport applications, loyalty programs, access control systems and closed loop payment systems. It fully complies with

the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

25 The MIFARE technology library MIFARE Plus EV2 features AES authentication, data encryption on RF channel, potential for multiple instances of the file system consisting of 16byte blocks arranged into sectors with each sector having its own access control keys and conditions.

26 MIFARE Plus EV2 has its own guidance documentation, listed in*Table 15: Guidance documentation*.

27 The hardware platform is not fully described in the present Security Target, all useful information can be found in its dedicated Platform Security Target *[PF-ST]*. Nevertheless, the related assets, assumptions, threats, objectives and SFRs are reproduced in this document.

1.6 TOE description

1.6.1 TOE hardware description

28 The ST31N600 A01 is described in the Platform Security Target *ST31N600 A01 Security Target for composition*.

29 Note that the usage of the hardware platform and associated firmware is not limited or constrained when MIFARE Plus EV2 is embedded. The functions provided by the Security IC platform remain normally accessible to the ES, as well as its life-cycle.

30 The only exception is the Library Protection Unit (LPU) of the hardware platform which is dedicated to the protection of MIFARE Plus EV2, ensuring that no application can read, write, compare any piece of data or code belonging to MFPEV2. Thus, the LPU is not available for any other usage.

1.6.2 TOE software description

31 The ST31N600 A01 firmware, included in the platform evaluation is described in the *ST31N600 A01 Security Target for composition*.

32 The TOE comprises a secure applicative Embedded Software, a MIFARE technology library, which is embedded in the User NVM of the Platform by ST, and protected for confidentiality and integrity of code and data by the LPU. MFPEV2 is used in the User configuration mode of the hardware platform.

33 MIFARE Plus® EV2 offers three different security levels. The higher the security level, the more secure the MFPEV2 Software is intended to be.
The main features of each security level are listed below:

- Security level 0 (SL0): The TOE does not provide any functionality besides initialization. The TOE is initialized in plaintext, especially keys for the further levels can be brought in. A TOE in SL0 is not usable for other purposes. After all mandatory keys and security attributes have been stored in the card, it can be switched to SL1 or SL3.
  Note: SL0 supports both ISO14443-3 and ISO1SO14443-4 protocol communication. ISO14443-3 communication is never in scope of the evaluation. Proximity Check,

Virtual Card Architecture are also out of scope. Personalization and Originality Check are in scope.

- Security level 1 (SL1): Different functionality is provided in ISO14443-3 and ISO14443-4 communication.
  In ISO14443-3 communication (the MIFARE Classic compatibility mode), the card user can access the blocks in the TOE after an authentication procedure, update the security attributes, update the authentication data. The communication with the terminal is protected, however the authentication and the protected communication in the security level are not evaluated security services of the TOE. This mode does not implement any Security Functional Requirement and is therefore not in the scope of the evaluation.
  In ISO14443-4 communication, the TOE can be switched to SL3, dedicated Sectors can be switched to SL3 or SL1SL3Mix. Both actions require preceding authentication using the AES algorithm with the appropriate key. In addition some security attributes and authentication data can be updated using SL3 commands. For sectors in SL3 or SL1SL3Mix, their sector trailer and keys can be updated using SL3 commands.
  Note: The only functionality provided by SL1 that is within the scope of the evaluation, is the Originality Check, updating security attributes and authentication data with SL3 command and the switching of the Card or Sector Security Level. Proximity Check, Virtual Card Architecture, data access of sectors in SL3 or SL1SL3Mix, are out of scope.
- Security level 3 (SL3): The card user can access the data and value blocks in the TOE after an authentication procedure based on the AES algorithm. The communication with the card terminal can be protected with secure messaging. The authentication and the secure messaging are security services of the TOE. The TOE cannot be switched to a different Security Level. In SL3, the TOE offers two secure messaging modes: EV0 Secure Messaging and EV1 Secure Messaging. Only the ISO14443-4 protocol is supported.
  Note: All functionality provided by Security Level 3 is within the scope of the evaluation, except Proximity Check .

34 In all security levels, the TOE does additionally support the so-called originality function which allows verifying the authenticity of the TOE.

35 For SL1 the SecurityLevel for the TOE as a whole, as well as the SectorSecurityLevels for dedicated Sectors can be switched to a higher level. A migration, both at TOE or at Sector level, is only possible to a higher level and not to a lower one. In case dedicated sectors have been migrated to higher Sector Security Levels, the overall TOE behavior must remain by default according to the lowest Sector Security Level among all Sectors of the TOE. If the TOE is in SL0, this must always hold for the whole TOE, which means that all Sectors are in Sector Security Level 0.

36 In MFPEV2, the TOE supports the virtual card architecture by providing a selection mechanism for virtual cards. This allows using the TOE in a complex environment where multiple virtual cards are stored in one physical object, however the TOE does support only one virtual card.

37 **Note**: The ES is not part of the TOE and is out of the scope of the evaluation, except MIFARE Plus EV2.

38 The TOE doesn’t need non-TOE hardware, software or firmware.

39 Note that the notion of various different roles and privileges does not exist for the MFPEV2 library. Only one role (the ES) is defined at the level of the MFPEV2 library and there are no privileges, the ES having access to all the functions of the MFPEV2 API.

1.6.3 TOE documentation

40 The user guidance documentation, part of the TOE, consists of:

- the platform user guidance documentation listed in the *ST31N600 A01 Security Target for composition*,
- the MIFARE Plus EV2 user manual,
- the MIFARE Plus EV2 interface specification,
- the MIFARE Plus EV2 release note.

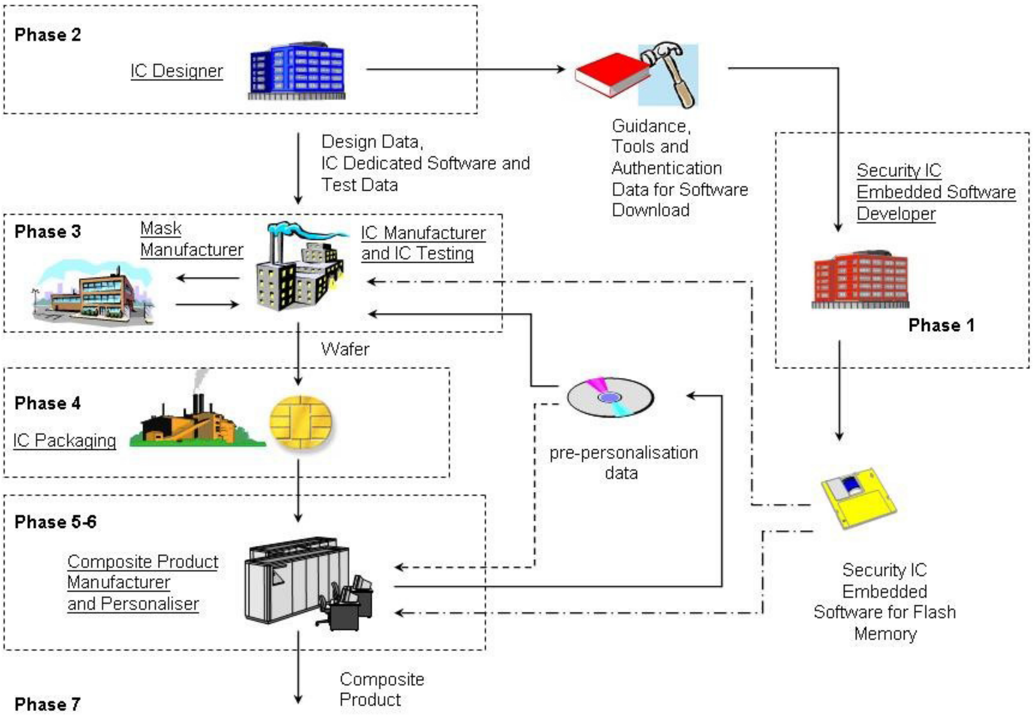
41 The complete list and details of guidance documents is provided in *Table 15*, except those of the platform, listed in the *ST31N600 A01 Security Target for composition*.

1.7 TOE life cycle

42 This Security Target is fully conform to the claimed PP. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 1.2.3.

43 The composite product life cycle is decomposed into 7 phases. Each of these phases has the very same boundaries as those defined in the claimed protection profile.

Figure 2. Security IC Life-Cycle


Phase 2
IC Designer
Guidance, Tools and Authentication Data for Software Download
Design Data, IC Dedicated Software and Test Data
Security IC Embedded Software Developer
Phase 1
Phase 3
Mask Manufacturer
IC Manufacturer and IC Testing
Wafer
Phase 4
IC Packaging
pre-personalisation data
Security IC Embedded Software for Flash Memory
Phase 5-6
Composite Product Manufacturer and Personaliser
Composite Product
Phase 7

44 The life cycle phases are summarized in *Table 2*.

45 The security IC platform life cycle is described in the Platform Security Target, as well as its delivery format.

46 All the sites likely to be involved in the complete TOE life cycle are listed in *Table 16*, except those dedicated to the Security IC platform, already detailed in the Platform Security Target. In *Table 16*, the library development centers are denoted by the activity “ES-DEV”. The IT support centers are denoted by the activity "IT".

47 MFPEV2 is developed as part of Phase 1, then embedded by ST in the User NVM of the platform, in Phase 3, in one of the sites denoted by the activity “EWS” in the Platform Security Target.

48 The TOE is then delivered as described in the Platform Security Target, i.e. after Phase 3 in form of wafers or after Phase 4 in packaged form, depending on the customer’s order.

49 In the following, the term "TOE delivery" is uniquely used to indicate:

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

50 The sites potentially involved in the complete TOE life cycle are listed in *Table 16*, except those dedicated to the Security IC platform, already detailed in the Platform Security Target.

Table 2. Composite product life cycle phases

Phase	Name	Description
1	IC embedded software development	security IC embedded software development specification of IC pre-personalization requirements
2	IC development	IC design IC dedicated software development
3	IC manufacturing	integration and photomask fabrication IC production IC testing Initialisation pre-personalisation if necessary
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary
5	Composite product integration	composite product finishing process
6	Personalisation	composite product personalisation composite product testing
7	Operational usage	composite product usage by its issuers and consumers

1.7.1 TOE intended usage

51 In Phase 7, the TOE is in the end-user environments. Depending on the application, the composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are secure contact-less transport applications and

related loyalty programs, access control systems, event ticketing, electronic voucher, closed loop payment systems.

52 The end-user environment therefore covers a wide range of very different functions. The TOE is designed to be used in unsecured and unprotected environments.

1.7.2 Delivery format and method

53 MIFARE Plus EV2 is delivered with the Security IC, already embedded by ST, in phase 3 or 4.

54 The Security IC platform can be delivered in form of wafers, micromodules or packages, as described in the *ST31N600 A01 Security Target for composition*.

55 All the possible forms of delivery are equivalent from a security point of view.

56 All the guidance documents are delivered as ciphered pdf files.

2 Conformance claims (ASE_CCL, ASE_ECD)

2.1 Common Criteria conformance claims

57 The MIFARE Plus EV2 on ST31N600 A01 Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

58 Furthermore it claims to be CC Part 2 (*CCMB-2017-04-002 R5*) extended and CC Part 3 (*CCMB-2017-04-003 R5*) conformant.

59 The extended Security Functional Requirements are all defined in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*):

- **FCS_RNG** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage,
- **FDP_SDC** Stored data confidentiality,
- **FIA_API** Authentication proof of identity.

The reader can find their certified definitions in the text of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*".

60 The assurance level for the MIFARE Plus EV2 on ST31N600 A01 Security Target is EAL5 augmented by ALC_DVS.2, AVA_VAN.5 and ALC_FLR.1.

61 The ST31N600 A01 platform has been evaluated according to the evaluation level EAL6 augmented by ALC_FLR.1, thus ensuring compatibility between the assurance levels chosen for the platform and this composite evaluation.

2.2 PP Claims

2.2.1 PP Reference

62 The MIFARE Plus EV2 on ST31N600 A01 Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), as required by this Protection Profile.

63 The following packages have been selected from the *BSI-CC-PP-0084-2014*, and completely addressed by the Security IC platform:

- Package “Authentication of the Security IC”,
- Packages for Loader:
  - Package 1: Loader dedicated for usage in Secured Environment only,
  - Package 2: Loader dedicated for usage by authorized users only.

2.2.2 PP Additions

64 The main additions operated on the *BSI-CC-PP-0084-2014* are:

- Those described in the *ST31N600 A01 Security Target for composition*,
- Specific additions for MFPEV2.

65 These additions are used to address additional functionality provided by the TOE, and not covered by the *Eurosmart - Security IC Platform Protection Profile with Augmentation*

Packages, nor by the Platform Security Target *ST31N600 A01 Security Target for composition*. They address the additional security functionality provided by MFPEV2.

66 All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-CC-PP-0084-2014* being typeset as indicated here and ~~here~~. Text originating in *[AUG]* is typeset as indicated here. Text originating in *[JILSR]* is typeset as indicated here.

67 The security environment additions relative to the PP are summarized in *Table 3*.

68 The additional security objectives relative to the PP are summarized in *Table 4*.

69 The additional SFRs for the TOE relative to the PP are summarized in *Table 6*.

70 The additional SARs relative to the PP are summarized in *Table 7*.

2.2.3 PP Claims rationale

71 The differences between this Security Target security objectives and requirements and those of *BSI-CC-PP-0084-2014*, to which conformance is claimed, have been identified and justified in *Section 4* and in *Section 5*. They have been introduced in the previous section.

72 In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the *BSI-CC-PP-0084-2014*.

73 The security problem definition presented in *Section 3*, clearly shows the additions to the security problem statement of the PP.

74 The security objectives rationale presented in *Section 4.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-CC-PP-0084-2014*.

75 Similarly, the security requirements rationale presented in *Section 5.4* has been updated with respect to the protection profile.

76 All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness have been argued in the rationale sections of the present document.

3 Security problem definition (ASE_SPD)

77 This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assets to be protected, the threats, the organisational security policies and the assumptions.

78 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security aspects defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security aspects have been introduced in the Platform Security Target and in this one.

79 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3.

80 A summary of all these security aspects with their respective origin and status of inclusion in the *ST31N600 A01 Security Target for composition* is provided in *Table 3*.
All the security aspects defined in the *ST31N600 A01 Security Target for composition* are valid for the present Security Target.

81 Only the ones introduced in this Security Target, are detailed in the following sections (column “In *[PF-ST]* ” = No).

Table 3. Summary of security aspects

	Label	Title	Origin	In *[PF-ST]*
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage	*[PP0084]*	Yes
	BSI.T.Phys-Probing	Physical Probing	*[PP0084]*	Yes
	BSI.T.Malfunction	Malfunction due to Environmental Stress	*[PP0084]*	Yes
	BSI.T.Phys-Manipulation	Physical Manipulation	*[PP0084]*	Yes
	BSI.T.Leak-Forced	Forced Information Leakage	*[PP0084]*	Yes
	BSI.T.Abuse-Func	Abuse of Functionality	*[PP0084]*	Yes
	BSI.T.RND	Deficiency of Random Numbers	*[PP0084]*	Yes
	BSI.T.Masquerade-TOE	Masquerade the TOE	*[PP0084]*	Yes
	AUG4.T.Mem-Access	Memory Access Violation	*[AUG]*	Yes
	JIL.T.Open-Samples-Diffusion	Diffusion of open samples	*[JILSR]*	Yes
	T.Data-Modification	Unauthorised data modification		No
	T.Impersonate	Impersonating authorised users during authentication		No
	T.Cloning	Cloning		No

Table 3. Summary of security aspects (continued)

	Label	Title	Origin	In *[PF-ST]*
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production	*[PP0084]*	Yes
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality	*[PP0084]*	Yes
	BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality	*[PP0084]*	Yes
	AUG1.P.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	P.Encryption	Confidentiality during communication		No
	P.MAC	Integrity during communication		No
	P.No-Trace	Un-traceability of end-users		No
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	*[PP0084]*	Yes
	BSI.A.Resp-Appl	Treatment of User Data	*[PP0084]*	Yes
	A.Secure-Values	Usage of secure values		No
	A.Terminal-Support	Terminal support		No

3.1 Description of assets

82 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), the high-level concerns defined in section 3.1 of the Protection Profile are related to standard functionality and are applied and the assets regarding threats are clarified in the *ST31N600 A01 Security Target for composition*.

- The user data of the Composite TOE,
- The Security IC Embedded Software, stored and in operation,
- The security services provided by the TOE for the Security IC Embedded Software.

83 These assets are related to the following high-level security concerns:

- Integrity of User Data of the composite TOE,
- Confidentiality of User Data of the composite TOE being stored in the TOE’s protected memory areas,
- Correct operation of the Security Services provided by the TOE for the Security IC Embedded Software,
- Deficiency of random numbers.

84 To be able to protect the assets based on this concerns, the TOE shall protect its security functionality. Therefore, critical information about the TOE shall be protected by the development environment and the operational environment. Critical information includes:

- Logical design data, physical design data, IC Dedicated Software, and configuration data.
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photomasks.

85 Note that the keys for the cryptographic co-processors are seen as User Data.

3.2 Threats

86 These threats are described in the Platform Security Target *[PF-ST]*, and just recalled here.

BSI.T.Leak-Inherent	Inherent Information Leakage
BSI.T.Phys-Probing	Physical Probing
BSI.T.Malfunction	Malfunction due to Environmental Stress
BSI.T.Phys-Manipulation	Physical Manipulation
BSI.T.Leak-Forced	Forced Information Leakage
BSI.T.Abuse-Func	Abuse of Functionality
BSI.T.RND	Deficiency of Random Numbers
BSI.T.Masquerade-TOE	Masquerade the TOE
AUG4.T.Mem-Access	Memory Access Violation
JIL.T.Open-Samples-Diffusion	Diffusion of open samples

87 The following additional threats are related to MFPEV2.

T.Data-Modification Unauthorised data modification:

User data stored by the TOE may be modified by unauthorised subjects. This threat applies to the processing of modification commands received by the TOE, it is not concerned with verification of authenticity.

T.Impersonate Impersonating authorised users during authentication:

An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the middle or replay attack.

T.Cloning Cloning:

User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.

3.3 Organisational security policies

88 These security policies are described in the Platform Security Target *[PF-ST]*, and just recalled here.

BSI.P.Process-TOE	Identification during TOE Development and Production
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality
AUG1.P.Add-Functions	Additional Specific Security Functionality

89 The TOE provides specific security functionality that can be used by MFPEV2. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the Security IC application, against which threats MFPEV2 will use the specific security functionality.

90 New Organisational Security Policies (OSPs) are defined here below:

91 P.Encryption, P.MAC and P.No-Trace are related to MFPEV2.

P.Encryption Confidentiality during communication:

The TOE shall provide the possibility to protect selected data elements from eavesdropping during contactless communication.

P.MAC Integrity during communication:

The TOE shall provide the possibility to protect the contactless communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session.

P.No-Trace Un-traceability of end-users:

The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised subjects without consent. Tracing of end-users may happen by performing a contactless communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element.

3.4 Assumptions

92 These assumptions are described in the Platform Security Target *[PF-ST]* and in the *BSI-CC-PP-0084-2014*, section 3.4.

BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
BSI.A.Resp-Appl	Treatment of User Data of the Composite TOE

93 The following assumptions are added for MFPEV2. They are required for the correct functioning of MFPEV2 security functionality.
They do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, since they are only related to assets which are out of the scope of this PP.

94 In consequence, the addition of these assumptions does not contradict with the strict conformance claim on the *BSI-CC-PP-0084-2014*.

A.Secure-Values

Usage of secure values:

Only confidential and secure cryptographically strong keys shall be used to set up the authentication. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal-Support

Terminal support:

The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. Furthermore, the terminal shall provide random numbers according to AIS20/31 *[1]* for the authentication

4 Security objectives (ASE_OBJ)

95 The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation during development and production phases,
- provide random numbers,
- provide access control functionality,
- provide cryptographic support.

96 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security objectives defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security objectives have been introduced in the Platform Security Target and in this one.

97 Note that the origin of each security objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3.

98 A summary of all the TOE security objectives with their respective origin and status of inclusion in the *ST31N600 A01 Security Target for composition* is provided in *Table 4*.
All the security objectives defined in the *ST31N600 A01 Security Target for composition* are valid for the present Security Target.

99 Only the ones introduced in this Security Target, are detailed in the following sections.

Table 4. Summary of security objectives

	Label	Title	Origin	In *[PF-ST]*
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage	*[PP0084]*	Yes
	BSI.O.Phys-Probing	Protection against Physical Probing	*[PP0084]*	Yes
	BSI.O.Malfunction	Protection against Malfunctions	*[PP0084]*	Yes
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation	*[PP0084]*	Yes
	BSI.O.Leak-Forced	Protection against Forced Information Leakage	*[PP0084]*	Yes
	BSI.O.Abuse-Func	Protection against Abuse of Functionality	*[PP0084]*	Yes
	BSI.O.Identification	TOE Identification	*[PP0084]*	Yes
	BSI.O.RND	Random Numbers	*[PP0084]*	Yes
	BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader	*[PP0084]*	Yes
	BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader	*[PP0084]*	Yes

Table 4. Summary of security objectives (continued)

	Label	Title	Origin	In *[PF-ST]*
TOE	JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF	*[JILSR]*	Yes
	JIL.O.Secure-Load-ACode	Secure loading of the Additional Code	*[JILSR]*	Yes
	JIL.O.Secure-AC-Activation	Secure activation of the Additional Code	*[JILSR]*	Yes
	JIL.O.TOE-Identification	Secure identification of the TOE	*[JILSR]*	Yes
	O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image	*[PF-ST]*	Yes
	O.MemImage-Identification	Secure identification of the Memory Image	*[PF-ST]*	Yes
	BSI.O.Authentication	Authentication to external entities	*[PP0084]*	Yes
	AUG1.O.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	AUG4.O.Mem-Access	Area based Memory Access Control	*[AUG]*	Yes
	O.Access-Control	Access Control		No
	O.Authentication	Authentication		No
	O.Encryption	Confidential Communication		No
	O.MAC	Integrity-protected Communication		No
	O.No-Trace	Preventing Traceability		No
	O.Type-Consistency	Data type consistency		No

Table 4. Summary of security objectives (continued)

	Label	Title	Origin	In *[PF-ST]*
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE	*[PP0084]*	Yes
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	*[PP0084]*	Yes
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	*[PP0084]*	Yes
	BSI.OE.Loader-Usage	Secure communication and usage of the Loader	*[PP0084]*	Yes
	BSI.OE.TOE-Auth	External entities authenticating of the TOE	*[PP0084]*	Yes
	OE.Composite-TOE-Id	Composite TOE identification	*[PF-ST]*	Yes
	OE.TOE-Id	TOE identification	*[PF-ST]*	Yes
	OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	*[PF-ST]*	Yes
	OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	*[PF-ST]*	Yes
	OE.Secure-Values	Generation of secure values		No
	OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers		No

4.1 Security objectives for the TOE

100 These security objectives are described in the Platform Security Target *[PF-ST]*

BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
BSI.O.Phys-Probing	Protection against Physical Probing
BSI.O.Malfunction	Protection against Malfunctions
BSI.O.Phys-Manipulation	Protection against Physical Manipulation
BSI.O.Leak-Forced	Protection against Forced Information Leakage
BSI.O.Abuse-Func	Protection against Abuse of Functionality
BSI.O.Identification	TOE Identification
BSI.O.RND	Random Numbers
BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader
BSI.O.Authentication	Authentication to external entities

JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF
JIL.O.Secure-Load-ACode	Secure loading of the Additional Code
JIL.O.Secure-AC-Activation	Secure activation of the Additional Code
JIL.O.TOE-Identification	Secure identification of the TOE
O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image
O.MemImage-Identification	Secure identification of the Memory Image
AUG4.O.Mem-Access	Area based Memory Access Control
AUG1.O.Add-Functions	Additional Specific Security Functionality

101 The following objectives are added for MFPEV2:

O.Access-Control

Access Control:
The TOE must provide an access control mechanism for application code and data stored by it. The access control mechanism shall apply to all operations for application elements and to reading and modifying security attributes. The cryptographic keys used for authentication shall never be output.

O.Authentication

Authentication:
The TOE must provide an authentication mechanism in order to be able to authenticate authorised users. The authentication mechanism shall be resistant against replay and man-in-the-middle attacks.

O.Encryption

Confidential Communication:
The TOE must be able to protect the communication by encryption. This shall be implemented by security attributes that enforce encrypted communication for the respective data elements.

O.MAC

Integrity-protected Communication:
The TOE must be able to protect the communication by adding a MAC. This shall be mandatory for commands that modify data on the TOE and optional on read commands. In addition a security attribute shall be available to mandate MAC on read commands, too. Usage of the protected communication shall also support the detection of injected and bogus commands within the communication session before the protected data transfer.

O.No-Trace

Preventing Traceability:
The TOE must be able to prevent that the TOE end-user can be traced. This shall be done by providing an option that disables the transfer of any information that is suitable for tracing an end-user by an unauthorised subject.

O.Type-Consistency

Data type consistency:
The TOE must provide a consistent handling of the different supported data types. This comprises over- and underflow checking for Values and Block sizes.

4.2 Security objectives for the environment

102 The following security objectives for the environment are detailed in the *ST31N600 A01 Security Target for composition* and still valid in the same terms for this Security Target. The clarifications made there also apply.

103 Security Objectives for the Security IC Embedded Software development environment (phase 1):

BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE

104 Security Objectives for the operational Environment (phase 4 up to 7):

BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	Up to phase 6
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	Up to phase 6
BSI.OE.Loader-Usage	Secure communication and usage of the Loader	Up to phase 7
BSI.OE.TOE-Auth	External entities authenticating of the TOE	Up to phase 7
OE.Composite-TOE-Id	Composite TOE identification	Up to phase 7
OE.TOE-Id	TOE identification	Up to phase 7
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	Up to phase 7
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	Up to phase 7

105 The following security objectives for the operational environment (phase 5 up to 7) are added for MFPEV2:

106 The TOE provides specific functionality that requires the TOE Manufacturer to implement measures for the unique identification of the TOE. Therefore, *OE.Secure-Values* is defined to allow a TOE specific implementation (refer also to *A.Secure-Values*).

107 The TOE provides specific functionality to verify the success of the application download process. Therefore, *OE.Terminal-Support* is defined to allow triggering the verification process.

OE.Secure-Values	Generation of secure values: The environment shall generate confidential and cryptographically strong secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalisation or usage in phase 5 to 7.

OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers: The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session.Furthermore, the terminal shall provide random numbers according to AIS20/31 *[1]* for the authentication.

4.3 Security objectives rationale

108 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* protection profile, those already introduced in the *ST31N600 A01 Security Target for composition* and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 3* are addressed by the security objectives stated in this chapter.

109 Thus, it is necessary to show that:

- security environment aspects from this ST, are addressed by security objectives stated in this chapter,
- security objectives from this ST, are suitable (i.e. they address security environment aspects),
- security objectives from this ST, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).

110 All security aspects are already justified in the Platform Security Target *[PF-ST]*, except the ones denoted by “New” in *Table 5*.

111 The augmentation made in this ST introduces the following security environment aspects:

- TOE threats "Unauthorised data modification, (*T.Data-Modification*)", "Impersonating authorised users during authentication, (*T.Impersonate*)", and "Cloning, (*T.Cloning*)",
- organisational security policies "Confidentiality during communication, (*P.Encryption*)", “Integrity during communication, (*P.MAC*)", and "Untraceability of end-users, (*P.No-Trace*)".
- assumptions "Usage of secure values, (*A.Secure-Values*)", and "Terminal support, (*A.Terminal-Support*)".

112 The justification of the additional policies, additional threats, and additional assumptions provided in the next subsections shows that they do not contradict to the rationale already given in the protection profile *BSI-CC-PP-0084-2014* and *ST31N600 A01 Security Target for composition* for the assumptions, policy and threats defined there.

113 In particular, the added assumptions do not contradict with the policies, threats and assumptions of the *BSI-CC-PP-0084-2014* Protection Profile, to which strict conformance is claimed, because they are all exclusively related to MFPEV2, which is out of the scope of this protection profile.

114 Only the security aspects denoted by “New” in *Table 5* will be detailed in the following.

Table 5. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func* *OE.Enable-Disable-Secure-Diag* *OE.Secure-Diag-Usage*	
BSI.T.RND	*BSI.O.RND*	
BSI.T.Masquerade-TOE	*BSI.O.Authentication* *BSI.OE.TOE-Auth*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
JIL.T.Open-Samples-Diffusion	*JIL.O.Prot-TSF-Confidentiality* *BSI.O.Leak-Inherent* *BSI.O.Leak-Forced*	
T.Data-Modification	*O.Access-Control* *O.Type-Consistency* *OE.Terminal-Support*	New
T.Impersonate	*O.Authentication*	New
T.Cloning	*O.Access-Control* *O.Authentication*	New
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	
BSI.P.Ctrl-Loader	*BSI.O.Ctrl-Auth-Loader* *JIL.O.Secure-Load-ACode* *JIL.O.Secure-AC-Activation* *JIL.O.TOE-Identification* *O.Secure-Load-AMemImage* *O.MemImage-Identification* *BSI.OE.Loader-Usage* *OE.TOE-Id* *OE.Composite-TOE-Id*	
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	

Table 5. Security Objectives versus Assumptions, Threats or Policies (continued)

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
P.Encryption	*O.Encryption*	New
P.MAC	*O.MAC*	New
P.No-Trace	*O.Access-Control* *O.Authentication* *O.No-Trace*	New
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
A.Secure-Values	*OE.Secure-Values*	New Phases 5-7
A.Terminal-Support	*OE.Terminal-Support*	New Phase 7

4.3.1 Assumption "Usage of secure values"

115 The justification related to the assumption “Usage of secure values, (*A.Secure-Values*)” is as follows:

116 *OE.Secure-Values* is an immediate transformation of this assumption, therefore it covers the assumption.

117 *A.Secure-Values* and *OE.Secure-Values* do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, because they are only related to MFPEV2, which is out of the scope of this protection profile.

4.3.2 Assumption "Terminal support"

118 The justification related to the assumption “Terminal support, (*A.Terminal-Support*)” is as follows:

119 The objective *OE.Terminal-Support* is an immediate transformation of the assumption, therefore it covers the assumption. The TOE can only check the integrity of data received from the terminal. For data transferred to the terminal, the receiver must verify the integrity of the received data. Furthermore the TOE cannot verify the entropy of the random number sent by the terminal. The terminal itself must ensure that random numbers are generated with appropriate entropy for the authentication. This is assumed by the related assumption, therefore the assumption is covered.

120 *A.Terminal-Support* and *OE.Terminal-Support* do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, because they are only related to MFPEV2, which is out of the scope of this protection profile.

4.3.3 TOE threat "Unauthorised data modification"

121 The justification related to the threat “Unauthorised data modification, (*T.Data-Modification*)” is as follows:

122 According to threat *T.Data-Modification*, the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective *O.Access-Control* requires an access control mechanism that limits the ability to modify data and code elements stored by the TOE. *O.Type-Consistency* ensures that data types are adhered, so that TOE data cannot be modified by abusing type-specific operations. The terminal must support this by checking the TOE responses, which is required by *OE.Terminal-Support*. Therefore *T.Data-Modification* is covered by these three objectives.

123 The added objectives for the TOE *O.Access-Control* and *O.Type-Consistency* do not introduce any contradiction in the security objectives for the TOE.

4.3.4 TOE threat "Impersonating authorised users during authentication"

124 The justification related to the threat “Impersonating authorised users during authentication, (*T.Impersonate*)” is as follows:

125 The threat is related to the fact that an unauthorised subject may try to impersonate an authorised subject during authentication, e.g. by a man-in-the middle or replay attack. *O.Authentication* requires that the authentication mechanism provided by the TOE shall be resistant against attack scenarios targeting the impersonation of authorized users. Therefore the threat is covered by *O.Authentication*.

126 The added objective for the TOE *O.Authentication* does not introduce any contradiction in the security objectives for the TOE.

4.3.5 TOE threat "Cloning"

127 The justification related to the threat “Cloning, (*T.Cloning*)” is as follows:

128 The concern of *T.Cloning* is that all data stored on the TOE (including keys) may be read out in order to create a duplicate.
O.Access-Control requires that unauthorized users can not read any information that is restricted to the authorized subjects. The cryptographic keys used for the authentication are stored inside the TOE and are protected by this objective. This objective states that no keys used for authentication shall ever be output. *O.Authentication* requires that users are authenticated before they can read any information that is restricted to authorized users. Therefore the two objectives cover *T.Cloning*.

4.3.6 Organisational security policy "Confidentiality during communication"

129 The justification related to the organisational security policy "Confidentiality during communication, (*P.Encryption*)” is as follows:

130 *O.Encryption* is an immediate transformation of the security policy, therefore it covers the Security Policy.

131 The added objective for the TOE *O.Encryption* does not introduce any contradiction in the security objectives.

4.3.7 Organisational security policy "Integrity during communication"

132 The justification related to the organisational security policy "Integrity during communication, (*P.MAC*)" is as follows:

133 *O.MAC* is an immediate transformation of the security policy, therefore it covers the Security Policy.

134 The added objective for the TOE *O.MAC* does not introduce any contradiction in the security objectives.

4.3.8 Organisational security policy "Untraceability of end-users"

135 The justification related to the organisational security policy "Untraceability of end-users, (*P.No-Trace*)" is as follows:

136 This policy requires that the TOE has the ability to prevent tracing of end-users. Tracing can be performed with the UID or with any freely accessible data element stored by the TOE.

137 *O.Access-Control* provides means to implement access control to data elements on the TOE and *O.Authentication* provides means to implement authentication on the TOE, in order to prevent tracing based on freely accessible data elements. *O.No-Trace* requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorized subject, which includes the UID. Therefore the policy is covered by these three objectives.

138 The added objective for the TOE *O.No-Trace* does not introduce any contradiction in the security objectives.

5 Security requirements (ASE_REQ)

139 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 5.1*), a section on security assurance requirements (SARs) for the TOE (*Section 5.2*), a section on the refinements of these SARs (*Section 5.3*) as required by the "*BSI-CC-PP-0084-2014*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 5.4*).

5.1 Security functional requirements for the TOE

140 The selected security functional requirements (SFRs) for this TOE (MIFARE Plus EV2 on ST31N600 A01) are summarized in *Table 6*.
This table also specifies:

- Their type i.e. drawn from *CCMB-2017-04-002 R5* or extended,
- Their origin i.e. defined in the *BSI-CC-PP-0084-2014* Protection Profile, in *[AUG]*, or in the Platform Security Target *[PF-ST]*. All SFRs are inherited from *[PF-ST]*, except those identified by “This ST”.

141 The extended SFRs are defined in the "*BSI-CC-PP-0084-2014*" Protection Profile.

142 All extensions to the SFRs of the "*BSI-CC-PP-0084-2014*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2017-04-002 R5*.

143 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2017-04-001 R5*. They are easily identified in the following text since they appear ***as indicated here***.

Table 6. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-CC-PP-0084-2014*	*CCMB-2017-04-002 R5*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality	*BSI-CC-PP-0084-2014*	Extended
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-CC-PP-0084-2014* Operated	

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing	*BSI-CC-PP-0084-2014* Operated	Extended
FDP_SDI.2	Stored data integrity monitoring and action			*CCMB-2017-04-002 R5*
FPT_PHP.3	Resistance to physical attack		*BSI-CC-PP-0084-2014*	
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1 / PTG.2	Random number generation / PTG.2	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	Extended
FCS_COP.1 / TDES	Cryptographic operation - TDES	Cipher scheme support	*[AUG]* #1 Operated / *[PF-ST]*	*CCMB-2017-04-002 R5*
FCS_COP.1 / AES	Cryptographic operation - AES			
FDP_ACC.1 / Memories	Subset access control	Memory access violation	*[PF-ST]*	
FDP_ACF.1 / Memories	Security attribute based access control		*[AUG]* #4 Operated	
FMT_MSA.3 / Memories	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Memories	Management of security attribute			
FMT_SMF.1 / Memories	Specification of management functions		*[PF-ST]*	
FIA_API.1	Authentication Proof of Identity	Masquerade	*BSI-CC-PP-0084-2014* Operated	Extended
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality		
FMT_LIM.2 / Loader	Limited availability			

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FTP_ITC.1 / Loader	Inter-TSF trusted channel - Loader	Loader violation	*BSI-CC-PP-0084-2014* Operated	*CCMB-2017-04-002 R5*
FDP_UCT.1 / Loader	Basic data exchange confidentiality - Loader			
FDP_UIT.1 / Loader	Data exchange integrity - Loader			
FDP_ACC.1 / Loader	Subset access control - Loader			
FDP_ACF.1 / Loader	Security attribute based access control - Loader			
FMT_MSA.3 / Loader	Static attribute initialisation - Loader	Correct Loader operation	*[PF-ST]*	
FMT_MSA.1 / Loader	Management of security attribute - Loader			
FMT_SMR.1 / Loader	Security roles - Loader			
FIA_UID.1 / Loader	Timing of identification - Loader			
FIA_UAU.1 / Loader	Timing of authentication - Loader			
FMT_SMF.1 / Loader	Specification of management functions - Loader			
FPT_FLS.1 / Loader	Failure with preservation of secure state - Loader			
FAU_SAR.1 / Loader	Audit review - Loader	Lack of TOE identification		
FAU_SAS.1 / Loader	Audit storage - Loader			Extended

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FTP_ITC.1 / Sdiag	Inter-TSF trusted channel - Secure Diagnostic	Abuse of Secure Diagnostic functionality	[PF-ST]	CCMB-2017-04-002 R5
FAU_SAR.1 / Sdiag	Audit review - Secure Diagnostic			
FMT_LIM.1 / Sdiag	Limited capabilities - Secure Diagnostic			Extended
FMT_LIM.2 / Sdiag	Limited availability - Secure Diagnostic			
FMT_SMR.1 / MFPEV2	Security roles	MFPEV2 access control policy	This ST	CCMB-2017-04-002 R5
FDP_ACC.1 / MFPEV2	Subset access control			
FDP_ACF.1 / MFPEV2	Security attribute based access control			
FMT_MSA.3 / MFPEV2	Static attribute initialisation			
FMT_MSA.1 / MFPEV2	Management of security attribute			
FMT_MTD.1 / MFPEV2	Management of TSF data			
FMT_SMF.1 / MFPEV2	Specification of management functions			
FDP_ITC.2 / MFPEV2	Import of user data with security attributes			

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FCS_COP.1 / MFPEV2-AES	Cryptographic operation - MFPEV2-AES	MFPEV2 confidentiality, authentication and integrity	This ST	CCMB-2017-04-002 R5
FCS_CKM.1 / MFPEV2	Cryptographic key generation			
FCS_CKM.4 / MFPEV2	Cryptographic key destruction			
FIA_UID.2 / MFPEV2	User identification before any action			
FIA_UAU.2 / MFPEV2	User authentication before any action			
FIA_UAU.3 / MFPEV2	Unforgeable authentication			
FIA_UAU.5 / MFPEV2	Multiple authentication mechanisms			
FTP_TRP.1 / MFPEV2	Trusted path			
FPT_TDC.1 / MFPEV2	Inter-TSF basic TSF data consistency			
FPT_RPL.1 / MFPEV2	Replay detection	MFPEV2 robustness		
FPR_UNL.1 / MFPEV2	Unlinkability			

144 All these SFRs have already been stated in the *ST31N600 A01 Security Target for composition*, and are satisfied by the *ST31N600* platform, except the following ones, dedicated to MFPEV2: *FMT_SMR.1 / MFPEV2*, *FDP_ACC.1 / MFPEV2*, *FDP_ACF.1 / MFPEV2*, *FMT_MSA.3 / MFPEV2*, *FMT_MSA.1 / MFPEV2*, *FMT_MTD.1 / MFPEV2*, *FMT_SMF.1 / MFPEV2*, *FDP_ITC.2 / MFPEV2*, *FCS_COP.1 / MFPEV2-AES*, *FCS_CKM.1 / MFPEV2*, *FCS_CKM.4 / MFPEV2*, *FIA_UID.2 / MFPEV2*, *FIA_UAU.2 / MFPEV2*, *FIA_UAU.3 / MFPEV2*, *FIA_UAU.5 / MFPEV2*, *FTP_TRP.1 / MFPEV2*, *FPT_TDC.1 / MFPEV2*, *FPT_RPL.1 / MFPEV2*, *FPR_UNL.1 / MFPEV2*.

145 The SFRs from the Platform Security Target are detailed in the *ST31N600 A01 Security Target for composition [PF-ST]*.

146 The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the capabilities and protections of MFPEV2.

5.1.1 Additional Security Functional Requirements regarding access control

Security roles (FMT_SMR.1) / MFPEV2

147 The TSF shall maintain the roles ***Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser, TransMACConfManager, Anybody and Nobody***.

148 The TSF shall be able to associate users with roles.

Subset access control (FDP_ACC.1) / MFPEV2

149 The TSF shall enforce the ***MFPEV2 Access Control Policy*** on ***all subjects, objects, operations and attributes defined by the MFPEV2 Access Control Policy.***

Security attribute based access control (FDP_ACF.1) / MFPEV2

150 The TSF shall enforce the ***MFPEV2 Access Control Policy*** to objects based on the following: ***all subjects, objects and attributes***.

151 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- ***In SL0 the Personaliser is allowed to perform Block.Write on all Blocks except Block 0.***
- ***In SL3 the CardUser is allowed to perform Block.Read and Block.Write for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.***
- ***In SL3 the CardUser is allowed to perform Value.Increase, Value.Decrease, Value.Transfer and Value.Restore for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.***

152 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

153 The TSF shall explicitly deny access of subjects to objects based on the following additional rules*:*

- ***No one but Nobody is allowed to perform Block.Write on Block 0 (first Block of the first Sector).***
- ***The OriginalityKeyUser is not allowed to perform any operation on objects.***

154 The following SFP ***MFPEV2 Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / MFPEV2":

155 *SFP_1: MFPEV2 Access Control Policy*

The Security Function Policy (SFP) MFPEV2 Access Control Policy uses the following definitions:

The defined subjects are:

- *Personaliser: Personaliser*
  The Personaliser is the subject that owns or has access to all cryptographic keys in

order to provide them to the TOE. Note that all actions performed by the Personaliser are restricted to SL0 and that those actions do not require an active authentication.

- *CardAdmin: Card Administrator*
  The CardAdmin is the subject that owns or has access to the CardMasterKey.
- *CardManager: Card Manager*
  The CardManager is the subject that owns or has access to the CardConfigurationKey.
- *SecurityLevelManager: Card Security level Manager*
  The SecurityLevelManager is the subject that owns or has access to the Level3SwitchKey.
- *SectorSecurityLevelManager: Sector Security level Manager*
  The SectorSecurityLevelManager is the subject that owns or has access to the Level3SectorSwitchKey and one or more AESSectorKeys.
- *CardUser: Card User*
  The CardUser is the subject that owns or has access to one or more AESSectorKeys. Note that the CardUser does not necessarily need to know both AESSectorKeys.KeyA and AESSectorKeys.KeyB of a particular Sector.
- *OriginalityKeyUser: Originality Key User*
  The OriginalityKeyUser is the subject that owns or has access to one or more OriginalityKeys.
- *TransMACConfManager: Transaction MAC Configuration Manager*
  The TransMACConfManager is the subject that owns or has access to one or more TransMACConfKeys.
- *Anybody: Anybody*
  Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser or TransMACConfManager, belongs to the role Anybody. This role includes the card holder (also referred to as end-user), and any other subject like an attacker for instance. The subjects belonging to Anybody do not possess any key and therefore are not able to perform any operation that is restricted to one of the roles which are explicitly excluded from the role Anybody.
- *Nobody: Nobody*
  Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser, TransMACConfManager or Anybody, belongs to the role Nobody. Due to the definition of Anybody, the set of all subjects belonging to the role Nobody is the empty set.

Note that multiple subjects may have the same role, e.g. for every Sector there are two CardUser (identified by the respective AESSectorKeys.KeyA and AESSectorKeys.KeyB for this Sector). The assigned rights to the CardUsers can be different, which allows having more or less powerful CardUser. There are also more than one OriginalityKeyUser and SecurityLevelManager.

The objects are:

- *Block: Block*
  Data is organized in Blocks of 16 bytes, which are accessed as elementary data units. Several instances of a Block are grouped into Sectors.
- *Sector: Sector*
  Each Sector consists of 4 or 16 Blocks.
- *SectorTrailer: Sector Trailer*
  The security attribute SectorTrailer is a specific Block that contains the access conditions for the corresponding Sector.
- *Value: Value*
  One specific type of data stored in a Block is called Value.
- *MFPConfigurationBlock: MFP Configuration Block*
  The security attribute MFPConfigurationBlock.
- *FieldConfigurationBlock: Field Configuration Block*
  The security attribute FieldConfigurationBlock.
- *SectorSecurityLevel: Sector Security Level*
  The sector security level of a designated Sector of the TOE.
- *SecurityLevel: Card Security Level*
  The security attribute SecurityLevel of the TOE.
- *CardMasterKey: Card Master Key*
  The key to manage keys and parameters for items of the TOE that do not require being changed in the field.
- *CardConfigurationKey: Card Configuration Key*
  The key to manage keys and parameters for items of the TOE that may require being changed in the field.
- *Level3SwitchKey: Level 3 Switch Key*
  Key to change SecurityLevel from SL1 to SL3.
- *Level3SectorSwitchKey: Level 3 Sector Switch Key*
  Key to switch dedicated Sectors from SectorSecurityLevel 1 to SectorSecurityLevel 3.
- *TransMACKey: Transaction MAC Key*
  Key to derive session keys that are used in the actual Transaction MAC computation. Note that there exists of four of these keys in total.
- *TransMACConfKey: Transaction MAC Configuration Key*
  Each TransMACKey is assigned a TransMACConfKey. An active authentication with the TransMACConfKey is required to enable the Transaction MAC feature for one or more dedicated Blocks.
- *TransMACConfBlock: Transaction MAC Configuration Block*
  Each TransMACKey is related with several TransMACConfBlocks.
- *AESSectorKeys: AES Sector Keys*
  The keys to manage access to Sectors. Since there are two keys for everySector the keys are called AESSectorKeys.KeyA and AESSectorKeys.KeyB.
- *OriginalityKey: Originality Key*
  The key to check the originality of the TOE.

The attributes are:

- *AESSectorKeys.KeyA: AES Sector key AESSectorKeys.KeyA.*
- *AESSectorKeys.KeyB: AES Sector key AESSectorKeys.KeyB.*

The operations that can be performed with the objects are:

- *Block.Read: Read data from a Block.*
- *Block.Write: Write data from a Block.*
- *SectorTrailer.Read: Read the security attribute SectorTrailer.*
- *SectorTrailer.Write: Write the security attribute SectorTrailer*
- *Value.Increase: Increase a Value.*
- *Value.Decrease: Decrease a Value.*
- *Value.Transfer: Transfer a Value.*
- *Value.Restore: Restore a Value.*
- *MFPConfigurationBlock.Modify: Modify the security attribute MFPConfigurationBlock..*
- *FieldConfigurationBlock.Modify: Modify the security attribute FieldConfigurationBlock..*
- *SectorSecurityLevel.Switch: Switch the SecurityLevel.*
- *CardMasterKey.Change: Change the CardMasterKey.*
- *CardConfigurationKey.Change: Change the CardConfigurationKey.*
- *Level3SwitchKey.Change: Change the Level3SwitchKey.*
- *Level3SectorSwitchKey.Change: Change the Level3SectorSwitchKey.*
- *TransMACKey.Change: Change the TransMACKey.*
- *TransMACConfKey.Change: Change the TransMACConfKey.*
- *TransMACConfBlock.Write: Write data to TransMACConfBlock.*
- *AESSectorKeys.Change: Change the AESSectorKeys.*
- *OriginalityKey.Change: Change the OriginalityKey.*

Note that subjects are authorised by cryptographic keys by appyling an authentication procedure. These keys are considered as authentication data and not as security attributes of the subjects.

Implications of the MFPEV2 Access Control Policy:

The MFPEV2 Access Control Policy has some implications, that can be drawn from the policy and that are essential parts of the TOE security functions.

- *The TOE end-user usually does not belong to the group of authorised users (consisting of CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser and OriginalityKeyUser), but is regarded as Anybody by the TOE. This means that the TOE cannot determine if it is used by its intended end-user (in other words: it cannot determine if the current card holder is the owner of the card).*
- *The Personaliser is very powerful, although the role is limited to SL0. The Personaliser is allowed to perform Block.Write on all Blocks and therefore change all data, all the keys (except the OriginalityKeys), and all SectorTrailers, MFPConfigurationBlocks and FieldConfigurationBlocks.*
- *Switching of the SecurityLevel is an integral part of the TOE security. The TOE is switched from SL0 to SL1 or SL3 at the end of the personalisation phase. Afterwards the SecurityLevel of the TOE can be increased by the SecurityLevelManager, the SectorSecurityLevels of dedicated Sectors of the TOE can be increased by the SectorSecurityLevelManager.*

Static attribute initialisation (FMT_MSA.3) / MFPEV2

156 The TSF shall enforce the ***MFPEV2 Access Control Policy*** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

157 The TSF shall allow the ***no one but Nobody*** to specify alternative initial values to override the default values when an object is created.

Management of security attributes (FMT_MSA.1) / MFPEV2

158 The TSF shall enforce the ***MFPEV2 Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***MFPConfigurationBlock, FieldConfigurationBlock, SectorTrailer and SecurityLevel*** to ***the Personaliser, CardManager, CardAdmin, SecurityLevelManager and CardUser***, ***respectively***.

159 ***Refinement:***

The detailed management abilities are:

- ***In SL0 the Personaliser is allowed to perform MFPConfigurationBlock.Modify.***
- ***In SL0 the Personaliser is allowed to perform FieldConfigurationBlock.Modify.***
- ***In SL0 the Personaliser is allowed to perform SectorTrailer.Modify.***
- ***In SL0 the Personaliser is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL1 or SL3.***
- ***The CardAdmin is allowed to perform MFPConfigurationBlock.Modify.***
- ***The CardManager is allowed to perform FieldConfigurationBlock.Modify.***
- ***In SL1 the SecurityLevelManager is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL3.***
- ***The CardUser is allowed to perform SectorTrailer.Read and SectorTrailer.Modify if the access conditions in the corresponding SectorTrailer grant him these rights.***

Management of TSF data (FMT_MTD.1) / MFPEV2

160 The TSF shall restrict the ability to ***modify*** the ***authentication data*** to ***the Personaliser, CardAdmin, CardManager, SecurityLevelManager and CardUser***.

161 ***Refinement:***

The detailed management abilities are:

- ***No one but Nobody is allowed to perform OriginalityKey.Change.***
- ***The Personaliser is allowed to perform CardMasterKey.Change.***
- ***The Personaliser is allowed to perform CardConfigurationKey.Change.***
- ***The Personaliser is allowed to perform Level3SwitchKey.Change.***
- ***The Personaliser is allowed to perform AESSectorKeys.Change.***
- ***The CardAdmin is allowed to perform CardMasterKey.Change.***
- ***The CardAdmin is allowed to perform Level3SwitchKey.Change.***
- ***The CardAdmin is allowed to perform Level3SectorSwitchKey.Change.***
- ***The CardAdmin is allowed to perform TransMACConfKey.Change.***
- ***The CardManager is allowed to perform CardConfigurationKey.Change.***
- ***The CardUser is allowed to perform AESSectorKeys.Change if the access conditions in the corresponding SectorTrailer grant him this right.***
- ***The TransMACConfManager is allowed to perform TransMACKey.Change.***

Specification of Management Functions (FMT_SMF.1) / MFPEV2

162 The TSF shall be capable of performing the following security management functions:

- ***Authenticating a user,***
- ***Invalidating the current authentication state based on the functions: Issuing a request for authentication, Occurrence of any error during the execution of a command, Reset, Switching the SecurityLevel of the TOE or the SectorSecurityLevel of dedicated Sectors, DESELECT according to ISO 14443-3, explicit authentication reset,***
- ***Finishing the personalisation phase by explicit request of the Personaliser***
- ***Changing a security attribute,***
- ***Selection and Deselection of the Virtual Card.***

Import of user data with security attributes (FDP_ITC.2) / MFPEV2

163 The TSF shall enforce the ***MFPEV2 Access Control Policy*** when importing user data, controlled under the SFP, from outside of the TOE.

164 The TSF shall use the security attributes associated with the imported user data.

165 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

166 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

167 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***no additional rules***.

5.1.2 Additional Security Functional Requirements regarding confidentiality, authentication and integrity

Cryptographic operation (FCS_COP.1) / MFPEV2-AES

The TSF shall perform ***encryption and decryption and cipher based MAC for authentication and communication*** in accordance with the specified algorithm ***Advanced Encryption Standard (AES) in one of the following modes of operation: CBC, CMAC*** and cryptographic key sizes ***128 bits*** that meet the following standards: *FIPS 197* ***(AES),*** *NIST SP 800-38A* ***(CBC mode),*** *NIST SP 800-38B* ***(CMAC mode)***.

168 ***Refinement:***
For the MIFARE Plus EV0 secure messaging the TOE uses the cryptographic algorithm for CBC according to NIST SP 800-38B (CBC mode) with the following modification: the TOE does not use an unpredictable IV, instead it uses a constructed IV which is partially predictable.

Cryptographic key generation (FCS_CKM.1) / MFPEV2

169 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***EV0 Session Key Generation and EV1 Session Key Generation*** and specified cryptographic key sizes ***128 bit*** that meets the following: ***MIFARE Plus EV2 interface specification - Technical note, section 3.7.2.1 AuthenticateFirst.***

Cryptographic key destruction (FCS_CKM.4) / MFPEV2

170 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***overwriting*** that meets the following: ***none***.

User identification before any action (FIA_UID.2) / MFPEV2

171 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

User authentication before any action (FIA_UAU.2) / MFPEV2

172 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Unforgeable authentication (FIA_UAU.3) / MFPEV2

173 The TSF shall ***detect and prevent*** use of authentication data that has been forged by any user of the TSF.

174 The TSF shall ***detect and prevent*** use of authentication data that has been copied from any user of the TSF.

Multiple authentication mechanisms (FIA_UAU.5) / MFPEV2

175 The TSF shall provide ***‘none’ and cryptographic authentication*** to support user authentication.

176 The TSF shall authenticate any user's claimed identity according to the ***following rules:***

- ***The ‘none’ authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The ‘none’ authentication implicitly and solely authenticates the Personaliser.***
- ***The cryptographic authentication is used in SL0 to authenticate the OriginalityKeyUser.***
- ***The cryptographic authentication is used in SL1 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager, the SecurityLevelManager, the SectorSecurityLevelManager and the CardUser.***
- ***The cryptographic authentication is used in SL3 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager, and the CardUser.***

Trusted path (FTP_TRP.1) / MFPEV2

177 The TSF shall provide a communication path between itself and ***remote*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***modification, disclosure or only modification***.

178 The TSF shall permit ***remote users*** to initiate communication via the trusted path.

179 The TSF shall require the use of the trusted path for ***authentication requests, confidentiality and/or integrity verification for data transfers, based on the setting in the MFPConfigurationBlock and the SectorTrailers***.

Inter-TSF basic TSF data consistency (FPT_TDC.1) / MFPEV2

180 The TSF shall provide the capability to consistently interpret ***data Blocks*** when shared between the TSF and another trusted IT product.

181 The TSF shall use ***the rules: data Blocks can always be modified by the Block.Write operation. If a data Block is in the data Value format it can be modified by all dedicated Value-specific operations honouring the Value-specific boundaries. SectorTrailers must have a specific format*** when interpreting the TSF data from another trusted IT product.

Application note:
The TOE does not interpret the contents of the data, e.g. it cannot determine if data stored in a specific Block is an identification number that adheres to a specific format. Instead the TOE distinguishes different types of Blocks and ensures that type-specific boundaries cannot be violated, e.g Values do not overflow. For SectorTrailers the TOE enforces a specific format.

5.1.3 Additional Security Functional Requirements regarding the robustness

Replay detection (FPT_RPL.1) / MFPEV2

182 The TSF shall detect replay for the following entities: ***authentication requests, confidentiality and/or integrity verification for data transfers based on the settings in the MFPConfigurationBlock and the SectorTrailers***.

183 The TSF shall perform ***rejection of the request*** when replay is detected.

Unlinkability (FPR_UNL.1) / MFPEV2

184 The TSF shall ensure that ***unauthorised subjects other than the card holder*** are unable to determine whether ***any operation of the TOE were caused by the same user***.

5.2 TOE security assurance requirements

185 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level ***5*** (EAL5) and augmented by taking the following components:

- ALC_DVS.2,
- AVA_VAN.5,
- ***ALC_FLR.1.***

186 Regarding application note 22 of *BSI-CC-PP-0084-2014*, the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

187 The component ALC_FLR.1 is chosen as an augmentation in this ST because a solid flaw management is key for the continuous improvement of the security IC platforms, especially on markets which need highly resistant and long lasting products.

188 The set of security assurance requirements (SARs) is presented in *Table 7*, indicating the origin of the requirement.

Table 7. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/*BSI-CC-PP-0084-2014*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	*BSI-CC-PP-0084-2014*
ALC_FLR.1	Basic flaw remediation	Security Target
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	EAL5/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_INT.1	ST introduction	EAL5/*BSI-CC-PP-0084-2014*
ASE_OBJ.2	Security objectives	EAL5/*BSI-CC-PP-0084-2014*
ASE_REQ.2	Derived security requirements	EAL5/*BSI-CC-PP-0084-2014*
ASE_SPD.1	Security problem definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_TSS.1	TOE summary specification	EAL5/*BSI-CC-PP-0084-2014*
ATE_COV.2	Analysis of coverage	EAL5/*BSI-CC-PP-0084-2014*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-CC-PP-0084-2014*
ATE_IND.2	Independent testing - sample	EAL5/*BSI-CC-PP-0084-2014*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-CC-PP-0084-2014*

5.3 Refinement of the security assurance requirements

189 As *BSI-CC-PP-0084-2014* defines refinements for selected SARs, these refinements are also claimed in this Security Target.

190 Regarding application note 23 of *BSI-CC-PP-0084-2014*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

191 An impact summary is provided in *Table 8*.

Table 8. Impact of EAL5 selection on *BSI-CC-PP-0084-2014* refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	4	None
ADV_ARC	1	1	None
ADV_FSP	4	5	None, presentation style changes
ADV_IMP	1	1	None
ATE_COV	2	2	None
AGD_OPE	1	1	None
AVA_VAN	5	5	None

5.4 Security Requirements rationale

5.4.1 Rationale for the Security Functional Requirements

192 Just as for the security objectives rationale of *Section* , the main line of this rationale is that the inclusion of all the security requirements of the *BSI-CC-PP-0084-2014* protection profile, together with those introduced in the Platform Security Target *[PF-ST]*, and those introduced in this Security Target, guarantees that all the security objectives identified in *Section 4* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

Table 9. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.LEAK-INHERENT	*Basic internal transfer protection FDP_ITT.1* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.PHYS-PROBING	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*
BSI.O.MALFUNCTION	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.PHYS-MANIPULATION	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*

Table 9. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* *Limited capabilities - Secure Diagnostic FMT_LIM.1 / Sdiag* *Limited availability - Secure Diagnostic FMT_LIM.2 / Sdiag* *Inter-TSF trusted channel - Secure Diagnostic FTP_ITC.1 / Sdiag* *Audit review - Secure Diagnostic FAU_SAR.1 / Sdiag* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FDP_SDI.2*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.O.Identification	*Audit storage FAU_SAS.1*
BSI.O.RND	*Random number generation / PTG.2 FCS_RNG.1 / PTG.2* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDI.2*, *FDP_SDC.1*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.OE.Resp-Appl	Not applicable
BSI.OE.Process-Sec-IC	Not applicable
BSI.OE.Lim-Block-Loader	Not applicable
BSI.OE.Loader-Usage	Not applicable
BSI.OE.TOE-Auth	Not applicable
OE.Enable-Disable-Secure-Diag	Not applicable
OE.Secure-Diag-Usage	Not applicable
BSI.O.Authentication	*Authentication Proof of Identity FIA_API.1*
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*

Table 9. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Ctrl-Auth-Loader	“*Inter-TSF trusted channel - Loader*” *FTP_ITC.1 / Loader* “*Basic data exchange confidentiality - Loader*” *FDP_UCT.1 / Loader* “*Data exchange integrity - Loader*” *FDP_UIT.1 / Loader* “*Subset access control - Loader*” *FDP_ACC.1 / Loader* “*Security attribute based access control - Loader*” *FDP_ACF.1 / Loader* “*Static attribute initialisation - Loader*” *FMT_MSA.3 / Loader* “*Management of security attribute - Loader*” *FMT_MSA.1 / Loader* “*Specification of management functions - Loader*” *FMT_SMF.1 / Loader* “*Security roles - Loader*” *FMT_SMR.1 / Loader* “*Timing of identification - Loader*” *FIA_UID.1 / Loader* “*Timing of authentication - Loader*” *FIA_UAU.1 / Loader*
JIL.O.Prot-TSF-Confidentiality	“*Inter-TSF trusted channel - Loader*” *FTP_ITC.1 / Loader* “*Basic data exchange confidentiality - Loader*” *FDP_UCT.1 / Loader* “*Data exchange integrity - Loader*” *FDP_UIT.1 / Loader* “*Subset access control - Loader*” *FDP_ACC.1 / Loader* “*Security attribute based access control - Loader*” *FDP_ACF.1 / Loader* “*Static attribute initialisation - Loader*” *FMT_MSA.3 / Loader* “*Management of security attribute - Loader*” *FMT_MSA.1 / Loader* “*Specification of management functions - Loader*” *FMT_SMF.1 / Loader* “*Security roles - Loader*” *FMT_SMR.1 / Loader* “*Timing of identification - Loader*” *FIA_UID.1 / Loader* “*Timing of authentication - Loader*” *FIA_UAU.1 / Loader*
JIL.O.Secure-Load-ACode	“*Inter-TSF trusted channel - Loader*” *FTP_ITC.1 / Loader* “*Basic data exchange confidentiality - Loader*” *FDP_UCT.1 / Loader* “*Data exchange integrity - Loader*” *FDP_UIT.1 / Loader* “*Subset access control - Loader*” *FDP_ACC.1 / Loader* “*Security attribute based access control - Loader*” *FDP_ACF.1 / Loader* “*Static attribute initialisation - Loader*” *FMT_MSA.3 / Loader* “*Management of security attribute - Loader*” *FMT_MSA.1 / Loader* “*Specification of management functions - Loader*” *FMT_SMF.1 / Loader* “*Security roles - Loader*” *FMT_SMR.1 / Loader* “*Timing of identification - Loader*” *FIA_UID.1 / Loader* “*Timing of authentication - Loader*” *FIA_UAU.1 / Loader* “*Audit storage - Loader*” *FAU_SAS.1 / Loader*
JIL.O.Secure-AC-Activation	“*Failure with preservation of secure state - Loader*” *FPT_FLS.1 / Loader*

Table 9. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
JIL.O.TOE-Identification	*“Audit storage - Loader” FAU_SAS.1 / Loader* *“Audit review - Loader” FAU_SAR.1 / Loader* *“Stored data integrity monitoring and action” FDP_SDI.2*
O.Secure-Load-AMemImage	*“Inter-TSF trusted channel - Loader” FTP_ITC.1 / Loader* *“Basic data exchange confidentiality - Loader” FDP_UCT.1 / Loader* *“Data exchange integrity - Loader” FDP_UIT.1 / Loader* *“Subset access control - Loader” FDP_ACC.1 / Loader* *“Security attribute based access control - Loader” FDP_ACF.1 / Loader* *“Static attribute initialisation - Loader” FMT_MSA.3 / Loader* *“Management of security attribute - Loader” FMT_MSA.1 / Loader* *“Specification of management functions - Loader” FMT_SMF.1 / Loader* *“Security roles - Loader” FMT_SMR.1 / Loader* *“Timing of identification - Loader” FIA_UID.1 / Loader* *“Timing of authentication - Loader” FIA_UAU.1 / Loader* *“Audit storage - Loader” FAU_SAS.1 / Loader*
O.MemImage-Identification	*“Failure with preservation of secure state - Loader” FPT_FLS.1 / Loader* *“Audit storage - Loader” FAU_SAS.1 / Loader* *“Audit review - Loader” FAU_SAR.1 / Loader* *“Stored data integrity monitoring and action” FDP_SDI.2*
OE.Composite-TOE-Id	Not applicable
OE.TOE-Id	Not applicable
AUG1.O.ADD-FUNCTIONS	*“Cryptographic operation - TDES” FCS_COP.1 / TDES* *“Cryptographic operation - AES” FCS_COP.1 / AES*
AUG4.O.MEM-ACCESS	*“Subset access control” FDP_ACC.1 / Memories* *“Security attribute based access control” FDP_ACF.1 / Memories* *“Static attribute initialisation” FMT_MSA.3 / Memories* *“Management of security attribute” FMT_MSA.1 / Memories* *“Specification of management functions” FMT_SMF.1 / Memories*
O.Access-Control	*“Cryptographic key destruction” FCS_CKM.4 / MFPEV2* *“Subset access control” FDP_ACC.1 / MFPEV2* *“Security attribute based access control” FDP_ACF.1 / MFPEV2* *“Import of user data with security attributes” FDP_ITC.2 / MFPEV2* *“Management of security attribute” FMT_MSA.1 / MFPEV2* *“Static attribute initialisation” FMT_MSA.3 / MFPEV2* *“Static attribute initialisation“ FMT_MTD.1 / MFPEV2* *“Specification of management functions” FMT_SMF.1 / MFPEV2* *“Security roles” FMT_SMR.1 / MFPEV2*

Table 9. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
O.Authentication	"*Cryptographic operation - MFPEV2-AES*" *FCS_COP.1 / MFPEV2-AES* "*Cryptographic key generation*" *FCS_CKM.1 / MFPEV2* "*User identification before any action*" *FIA_UID.2 / MFPEV2* "*User authentication before any action*" *FIA_UAU.2 / MFPEV2* "*Unforgeable authentication*" *FIA_UAU.3 / MFPEV2* "*Multiple authentication mechanisms*" *FIA_UAU.5 / MFPEV2* "*Specification of management functions*" *FMT_SMF.1 / MFPEV2* "*Replay detection*" *FPT_RPL.1 / MFPEV2* "*Trusted path*" *FTP_TRP.1 / MFPEV2*
O.Encryption	"*Cryptographic key generation*" *FCS_CKM.1 / MFPEV2* "*Cryptographic key destruction*" *FCS_CKM.4 / MFPEV2* "*Cryptographic operation - MFPEV2-AES*" *FCS_COP.1 / MFPEV2-AES* "*Trusted path*" *FTP_TRP.1 / MFPEV2*
O.MAC	"*Cryptographic key generation*" *FCS_CKM.1 / MFPEV2* "*Cryptographic key destruction*" *FCS_CKM.4 / MFPEV2* "*Cryptographic operation - MFPEV2-AES*" *FCS_COP.1 / MFPEV2-AES* "*Replay detection*" *FPT_RPL.1 / MFPEV2* "*Trusted path*" *FTP_TRP.1 / MFPEV2*
O.Type-Consistency	"*Inter-TSF basic TSF data consistency*" *FPT_TDC.1 / MFPEV2*
O.No-Trace	"*Unlinkability*" *FPR_UNL.1 / MFPEV2*
OE.Secure-Values	Not applicable
OE.Terminal-Support	Not applicable

193 All justifications for Security Objectives and SFRs have been already provided in the Platform Security Target *[PF-ST]*, except for *O.Access-Control, O.Authentication, O.Encryption*, *O.MAC, O.Type-Consistency*, *O.Access-Control,* and their associated SFRs.

194 This rationale must show that security requirements suitably address these objectives.

195 The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in *BSI-CC-PP-0084-2014* and in *[PF-ST]*, they form an internally consistent whole, is provided in the next subsections.

5.4.2 Additional security objectives are suitably addressed

Security objective "Access control for MFPEV2 (*O.Access-Control*)"

196 The justification related to the security objective "Access control for MFPEV2 (*O.Access-Control*)" is as follows:

197 The security functional requirement "*Security roles (FMT_SMR.1) / MFPEV2*" defines the roles of the MFPEV2 Access Control Policy.
The security functional requirements "*Subset access control (FDP_ACC.1) / MFPEV2*" and "*Security attribute based access control (FDP_ACF.1) / MFPEV2*" define the rules and "*Static attribute initialisation (FMT_MSA.3) / MFPEV2*" and "*Management of security attributes (FMT_MSA.1) / MFPEV2*" the attributes that the access control is based on.
The security functional requirement "*Management of TSF data (FMT_MTD.1) / MFPEV2*" provides the rules for the management of the authentication data.
The management functions are defined by "*Specification of Management Functions (FMT_SMF.1) / MFPEV2*".
Since the TOE stores data on behalf of the authorised subjects, import of user data with security attributes is defined by "*Import of user data with security attributes (FDP_ITC.2) / MFPEV2*".
Since cryptographic keys are used for authentication (refer to *O.Authentication*), these keys have to be removed if they are no longer needed for the access control (i.e. an application is deleted). This is required by "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*".
These nine SFRs together provide an access control mechanism as required by the objective *O.Access-Control*.

Security objective “Authentication for MFPEV2 (*O.Authentication*)”

198 The justification related to the security objective “Authentication for MFPEV2 (*O.Authentication*)” is as follows:

199 The security functional requirement "*Cryptographic operation (FCS_COP.1) / MFPEV2-AES*" requires that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication.
The security functional requirement "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*" generates the session key used after the authentication.
The security functional requirements "*User identification before any action (FIA_UID.2) / MFPEV2*", "*User authentication before any action (FIA_UAU.2) / MFPEV2*" and "*Unforgeable authentication (FIA_UAU.3) / MFPEV2*" together define that users must be identified and authenticated before any action. The security functional requirement "*Unforgeable authentication (FIA_UAU.3) / MFPEV2*" prevents that forged authentication data can be used.The ‘none’ authentication of "*Unforgeable authentication (FIA_UAU.3) / MFPEV2*" also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE.
"*Specification of Management Functions (FMT_SMF.1) / MFPEV2*" defines security management functions the TSF shall be capable to perform.
"*Trusted path (FTP_TRP.1) / MFPEV2*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 especially requires “authentication requests”.
Together with "*Replay detection (FPT_RPL.1) / MFPEV2*" which requires a replay detection for these authentication requests, the nine security functional requirements fulfill the objective *O.Authentication*.

Security objective “MFPEV2 Confidential Communication (*O.Encryption*)”

200 The justification related to the security objective “MFPEV2 Confidential communication (*O.Encryption*)” is as follows:

201 The security functional requirement "*Cryptographic operation - MFPEV2-AES*" requires that the TOE provides the basic cryptographic algorithm AES that can be used to protect the communication by encryption.
"*Trusted path (FTP_TRP.1) / MFPEV2*" requires a trusted communication path between the

TOE and remote users; FTP_TRP.1.3 especially requires “confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes”.
The security functional requirement "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*" generates the session key used for encryption. "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*" requires that cryptographic keys used for encryption have to be removed after usage.
These four security functional requirements fulfill the objective *O.Encryption*.

Security objective “MFPEV2 Integrity-protected Communication (*O.MAC*)”

202 The justification related to the security objective “MFPEV2 Integrity-protected Communication (*O.MAC*)” is as follows:

203 The security functional requirement "*Cryptographic operation - MFPEV2-AES*" requires that the TOE provides the basic cryptographic algorithms that can be used to compute a MAC which can protect the integrity of the communication.
"*Trusted path (FTP_TRP.1) / MFPEV2*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 especially requires “confidentiality and/or data integrity verification for data transfers on request of the file owner”.
The security functional requirement "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*" generates the session key used for the calculation. "*Cryptographic key generation (FCS_CKM.1) / MFPEV2*" requires that cryptographic keys used for MAC operations have to be removed after usage.
Replay detection (FPT_RPL.1) / MFPEV2 requires a replay detection for these data transfers.
These five security functional requirements fulfill the objective *O.MAC*.

Security objective “MFPEV2 Data type consistency (*O.Type-Consistency*)”

204 The justification related to the security objective “MFPEV2 Data type consistency (*O.Type-Consistency*)” is as follows:

205 The security functional requirement "*Inter-TSF basic TSF data consistency (FPT_TDC.1) / MFPEV2*" requires the TOE to consistently interpret data files and values. The TOE will honor the respective file formats and boundaries (i.e. upper and lower limits, size limitations). This meets the objective *O.Type-Consistency*.

Security objective “Preventing traceability for MFPEV2 (*O.Access-Control*)”

206 The justification related to the security objective “Preventing traceability for MFPEV2 (*O.Access-Control*)” is as follows:

207 The security functional requirement "*Unlinkability (FPR_UNL.1) / MFPEV2*" requires that unauthorised subjects other than the card holder are unable to determine whether any operation of the TOE were caused by the same user. This meets the objective *O.Access-Control*.

5.4.3 Additional security requirements are consistent

"Cryptographic key destruction (*FCS_CKM.4 / MFPEV2*),
Subset access control (*FDP_ACC.1 / MFPEV2*),
Security attribute based access control (*FDP_ACF.1 / MFPEV2*),
Import of user data with security attributes (*FDP_ITC.2 / MFPEV2*),
Management of security attributes (*FMT_MSA.1 / MFPEV2*),
Static attribute initialisation (*FMT_MSA.3 / MFPEV2*),
Management of TSF data (*FMT_MTD.1 / MFPEV2*),
Specification of management function (*FMT_SMF.1 / MFPEV2*),
Security roles (*FMT_SMR.1 / MFPEV2*)"

208 These security requirements have already been argued in *Section : Security objective “Access control for MFPEV2 (O.Access-Control)”* above.

" User authentication before any action (*FIA_UAU.2 / MFPEV2*),
Unforgeable authentication (*FIA_UAU.3 / MFPEV2*),
Multiple authentication mechanisms (*FIA_UAU.5 / MFPEV2*),
User identification before any action (*FIA_UID.2 / MFPEV2*)"

209 These security requirements have already been argued in *Section : Security objective “Authentication for MFPEV2 (O.Authentication)”* above.

"Cryptographic operation (*FCS_COP.1 / MFPEV2-AES*),
Cryptographic key generation (*FCS_CKM.1 / MFPEV2*),
Trusted path (*FTP_TRP.1 / MFPEV2*),
Replay detection (*FPT_RPL.1 / MFPEV2*)"

210 These security requirements have already been argued in *Section : Security objective “MFPEV2 Integrity-protected Communication (O.MAC)”* above.

"Inter-TSF basic TSF data consistency (*FPT_TDC.1 / MFPEV2*)"

211 This security requirement has already been argued in *Section : Security objective “MFPEV2 Data type consistency (O.Type-Consistency)”* above.

"Unlinkability (*FPR_UNL.1 / MFPEV2*)"

212 This security requirement has already been argued in *Section : Security objective “Preventing traceability for MFPEV2 (O.Access-Control)”* above.

5.4.4 Dependencies of Security Functional Requirements

213 All dependencies of Security Functional Requirements have been fulfilled in this Security Target except :

- those justified in the *BSI-CC-PP-0084-2014* protection profile security requirements rationale,
- those justified in the *ST31N600 A01 Security Target for composition [PF-ST]* security requirements rationale,
- those justified in *[AUG]* security requirements rationale.

214 Details are provided in *Table 10* below.

215 Note that in order to avoid repetitions of the SFRs iterated in this Security Target, and improve readability, some are mentioned in a generic form in this table.

Table 10. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-CC-PP-0084-2014*
FPT_FLS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Test	FMT_LIM.2 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Test	FMT_LIM.1 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Loader	FMT_LIM.2 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Loader	FMT_LIM.1 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Stest	FMT_LIM.2 / Stest	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Stest	FMT_LIM.1 / Stest	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Sdiag	FMT_LIM.2 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Sdiag	FMT_LIM.1 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*
FAU_SAS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDC.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDI.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FPT_PHP.3	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes, by FDP_ACC.1 / Memories and FDP_IFC.1	Yes, *BSI-CC-PP-0084-2014*
FPT_ITT.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-CC-PP-0084-2014*	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PTG.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FCS_CKM.1, see *[PF-ST]*	Yes, *[AUG]* ***#1***
	FCS_CKM.4	No, see *[PF-ST]*	
FCS_CKM.1	[FDP_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.1	
	FCS_CKM.4	No, see *[PF-ST]*	
FDP_ACC.1 / Memories	FDP_ACF.1 / Memories	Yes	Yes, *[PF-ST]*

Table 10. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes, by FDP_ACC.1 / Memories	Yes, *[PF-ST]*
	FMT_MSA.3 / Memories	Yes	
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No, see *[AUG]* ***#4***	
FMT_MSA.1 / Memories	[FDP_ACC.1 / Memories or FDP_IFC.1]	Yes, by FDP_ACC.1 / Memories and FDP_IFC.1	Yes, *[PF-ST]*
	FMT_SMF.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No	Yes, *[PF-ST]*
FMT_SMF.1 / Memories	None	No dependency	Yes, *[PF-ST]*
FIA_API.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FTP_ITC.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_UCT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_UIT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_MSA.3 / Loader	Yes	

Table 10. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	Yes, *[PF-ST]*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FIA_UID.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FIA_UAU.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_SMF.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FPT_FLS.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FAU_SAS.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FAU_SAR.1 / Loader	FAU_GEN.1	No, by FAU_SAS.1 / Loader instead, see *[PF-ST]*	Yes, *[PF-ST]*
FTP_ITC.1 / Sdiag	None	No dependency	Yes, *[PF-ST]*
FAU_SAR.1 / Sdiag	FAU_GEN.1	No, see *[PF-ST]*	Yes, *[PF-ST]*
FMT_SMR.1 / MFPEV2	FIA_UID.1 / MFPEV2	Yes, by FIA_UID.2 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
FDP_ACC.1 / MFPEV2	FDP_ACF.1 / MFPEV2	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / MFPEV2	FDP_ACC.1 / MFPEV2	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / MFPEV2	Yes	
FMT_MSA.3 / MFPEV2	FMT_MSA.1 / MFPEV2	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / MFPEV2	Yes	

Table 10. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FMT_MSA.1 / MFPEV2	[FDP_ACC.1 / MFPEV2 or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMF.1 / MFPEV2	Yes	
	FMT_SMR.1 / MFPEV2	Yes	
FMT_SMF.1 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FDP_ITC.2 / MFPEV2	[FDP_ACC.1 / MFPEV2 or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
	[FTP_ITC.1 or FTP_TRP.1 / MFPEV2]	Yes, by FTP_TRP.1 / MFPEV2	
	FPT_TDC.1 / MFPEV2	Yes	
FPT_TDC.1 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UID.2 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.2 / MFPEV2	FIA_UID.1	Yes, by FIA_UID.2 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.3 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.5 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FMT_MTD.1 / MFPEV2	FMT_SMR.1 / MFPEV2	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMF.1 / MFPEV2	Yes	
FTP_TRP.1 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FCS_COP.1 / MFPEV2-AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FCS_CKM.1 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
	FCS_CKM.4	Yes, by FCS_CKM.4 / MFPEV2	

Table 10. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FCS_CKM.1 / MFPEV2	[FCS_CKM.2 or FCS_COP.1]	Yes, by FDP_COP.1 / MFPEV2-AES	***No,*** *CCMB-2017-04-002 R5*
	FCS_CKM.4]	Yes, by FCS_CKM.4 / MFPEV2	
FCS_CKM.4 / MFPEV2	[FDP_ITC.1 or FDP_ITC.2 / MFPEV2 or FCS_CKM.1]	Yes, by FDP_ITC.2 / MFPEV2	***No,*** *CCMB-2017-04-002 R5*
FPT_RPL.1 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FPR_UNL.1 / MFPEV2	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

5.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5

216 Regarding application note 22 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

217 EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, extensive testing, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.

218 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

219 Note that detailed and updated refinements for assurance requirements are given in *Section 5.3*.

Dependencies of assurance requirements

220 Dependencies of security assurance requirements are fulfilled by the EAL5 package selection.

221 The augmentation to this package identified in *Section 5.2* does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_DVS.2 and AVA_VAN.5 dependencies have been justified in *BSI-CC-PP-0084-2014*,
- ALC_FLR.1 has no dependency.

6 TOE summary specification (ASE_TSS)

222 This section demonstrates how the TOE meets each Security Functional Requirement, and includes a statement of compatibility vs. the Platform Security Target *[PF-ST]*.

6.1 TOE Security Functional Requirements realisation

223 This section argues how the TOE meets each SFR.

224 The TOE is evaluated as a composite TOE, made of the underlying hardware platform and the MIFARE Plus EV2 library on top of it.

225 Consequently, the *ST31N600 A01 Security Target for composition* details how all the platform SFRs are met, and in the following only the SFRs related to MFPEV2 are addressed.

6.1.1 Security roles (FMT_SMR.1) / MFPEV2

226 MFPEV2 identifies the user to be authenticated by the key block number indicated in the authentication request.

227 In security level 0 when the TOE is in a secure environment, MFPEV2 identifies and authenticates the role Personaliser by default; in addition the role Originality Key User can be identified with an explicit authentication request.

228 In the other security levels, MFPEV2 identifies and authenticates the role Anybody by default and before any authentication request.
The roles Card Administrator, Card Manager, Card Security Level Manager, Card User and Originality Key User are authenticated during the authentication request by the knowledge of the respective cryptographic keys.

6.1.2 Subset access control (FDP_ACC.1) / MFPEV2

229 For each MFPEV2 command subject to access control, the MFPEV2 library verifies if the MFPEV2 access conditions are satisfied and returns an error when this is not the case.

6.1.3 Security attribute based access control (FDP_ACF.1) / MFPEV2

230 The MFPEV2 library verifies the MFPEV2 security attributes during the execution of MFPEV2 commands to enforce the MFPEV2 Access Control Policy defined by the MFPEV2 interface specification:

231 MFPEV2 assigns Card Users to 2 different groups of operations on blocks. The operations are "read" or "write".
There are several sets of predefined access conditions which may be assigned to each sector. These sets can also contain the access condition "never" for one group of operations. Card Users can also modify the sector trailer or the AES sector keys, if the access conditions allow this.

232 The Originality Key User is not allowed to perform any action on objects, but with a successful authentication he can prove the authenticity of the Card.

233 The Card Administrator can change the Level 3 Switch Key and the Card Master Key.

234 The Card Manager can modify the Field Configuration Block, which are attributes that may have to be changed in the field. He is also allowed to change the Card Configuration Key.

235 The Card Security Level Manager can switch the security level of the card to level 3 by authenticating with the corresponding key.

6.1.4 Static attribute initialisation (FMT_MSA.3) / MFPEV2

236 The MFPEV2 library initialises all the static attributes to the values defined by MFPEV2 interface specifications before they can be used by the Embedded Software.

6.1.5 Management of security attributes (FMT_MSA.1) / MFPEV2

237 The MFPEV2 library verifies the MFPEV2 security attributes during the execution of MFPEV2 commands to enforce the Access Control Policy on the security attributes.

6.1.6 Specification of Management Functions (FMT_SMF.1) / MFPEV2

238 The MFPEV2 library implements the management functions defined by the MFPEV2 interface specifications for authentication, and changing security attributes.

6.1.7 Import of user data with security attributes (FDP_ITC.2) / MFPEV2

239 The MFPEV2 library implements the MFPEV2 interface specifications and enforces the Access Control Policy to associate the user data to the security attributes.

6.1.8 Inter-TSF basic TSF data consistency (FPT_TDC.1) / MFPEV2

240 The MFPEV2 library implements the MFPEV2 interface specifications, supporting consistent interpretation and modification control of inter-TSF exchanges.

6.1.9 Cryptographic operation (FCS_COP.1) / MFPEV2-AES

241 The MFPEV2 library uses AES as cryptographic operation (AES accelerator), to perform encryption and decryption and cipher based MAC for authentication and communication in accordance with *FIPS 197, NIST SP 800-38A* and *NIST SP 800-38B*, in one of the following modes of operation: CBC, CMAC with a cryptographic key size of 128 bits.

242 Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

6.1.10 Cryptographic key generation (FCS_CKM.1) / MFPEV2

243 The MFPEV2 library generates session keys after a successful authentication.

6.1.11 Cryptographic key destruction (FCS_CKM.4) / MFPEV2

244 The MFPEV2 library erases key values from memory after their context becomes obsolete.

6.1.12 User identification before any action (FIA_UID.2) / MFPEV2

245 The MFPEV2 library identifies the user through the key selected for authentication as specified by the MFPEV2 Interface Specification.

6.1.13 User authentication before any action (FIA_UAU.2) / MFPEV2

246 During the authentication, the MFPEV2 library verifies that the user knows the selected key.

247 After this authentication, both parties share a session key.

6.1.14 Unforgeable authentication (FIA_UAU.3) / MFPEV2

248 During the authentication, the MFPEV2 library verifies knowledge of a secret key by applying it on a freshly generated random challenge.

6.1.15 Multiple authentication mechanisms (FIA_UAU.5) / MFPEV2

249 The MFPEV2 library implements the MFPEV2 Interface Specification, that has a mechanism to authenticate Card Administrator, Card Manager, Card Security Level Manager, Card User, and Originality Key User, while Everybody is assumed when there is no valid authentication state.

6.1.16 Management of TSF data (FMT_MTD.1) / MFPEV2

250 The MFPEV2 library implements the MFPEV2 Interface Specification, restricting key modifications in ways configurable through the security attributes to authenticated users, or disabling key modification capabilities.

6.1.17 Trusted path (FTP_TRP.1) / MFPEV2

251 The MFPEV2 library implements the MFPEV2 Interface Specification allowing to establish and enforce a trusted path between itself and remote users.

6.1.18 Replay detection (FPT_RPL.1) / MFPEV2

252 The MFPEV2 library implements the MFPEV2 authentication command, and authenticated commands, that allow replay detection.

6.1.19 Unlinkability (FPR_UNL.1) / MFPEV2

253 MFPEV2 provides an Administrator option to use random UID during the ISO 14443 anti-collision sequence, preventing the traceability through UID. At higher level, the MFPEV2 access control - when configured for this purpose - provides traceability protection.

6.2 Statement of compatibility

254 This section details the statement of compatibility between this Security Target and the Platform Security Target *[PF-ST]*.

255 The following mappings regarding SFRs, objectives and assurance requirements demonstrate that there is no inconsistency between this composite Security Target and the *ST31N600 A01 Security Target for composition*.

6.2.1 Compatibility of security objectives

256 There is no conflict between the security objectives of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 11. Platform Security Objectives vs. TOE Security Objectives

Platform Security Objectives	TOE Security Objectives
BSI.O.Leak-Inherent	*BSI.O.Leak-Inherent*
BSI.O.Phys-Probing	*BSI.O.Phys-Probing*
BSI.O.Malfunction	*BSI.O.Malfunction*
BSI.O.Phys-Manipulation	*BSI.O.Phys-Manipulation*
BSI.O.Leak-Forced	*BSI.O.Leak-Forced*
BSI.O.Abuse-Func	*BSI.O.Abuse-Func*
BSI.O.Identification	*BSI.O.Identification*
BSI.O.RND	*BSI.O.RND*
BSI.O.Authentication	*BSI.O.Authentication*
BSI.O.Cap-Avail-Loader	*BSI.O.Cap-Avail-Loader*
BSI.O.Ctrl-Auth-Loader	*BSI.O.Ctrl-Auth-Loader*
JIL.O.Prot-TSF-Confidentiality	*JIL.O.Prot-TSF-Confidentiality*
JIL.O.Secure-Load-ACode	*JIL.O.Secure-Load-ACode*
JIL.O.Secure-AC-Activation	*JIL.O.Secure-AC-Activation*
JIL.O.TOE-Identification	*JIL.O.TOE-Identification*
O.Secure-Load-AMemImage	*O.Secure-Load-AMemImage*
O.MemImage-Identification	*O.MemImage-Identification*
AUG1.O.Add-Functions	*AUG1.O.Add-Functions* *O.Authentication* *O.Encryption* *O.MAC*
AUG4.O.Mem-Access	*AUG4.O.Mem-Access*
	Additional objectives:
	O.Access-Control
	O.Authentication
	O.Encryption
	O.MAC
	O.Type-Consistency
	O.No-Trace

257 There is no conflict between the security objectives for the environment of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 12. Platform Security Objectives for the Environment vs. TOE Security Objectives for the Environment

Platform Security Objectives for the Environment	TOE Security Objectives for the Environment
BSI.OE.RESP-APPL	*BSI.OE.RESP-APPL*
BSI.OE.PROCESS-SEC-IC	*BSI.OE.PROCESS-SEC-IC*
BSI.OE.LIM-BLOCK-LOADER	*BSI.OE.LIM-BLOCK-LOADER*
BSI.OE.LOADER-USAGE	*BSI.OE.LOADER-USAGE*
BSI.OE.TOE-Auth	*BSI.OE.TOE-Auth*
OE.Enable-Disable-Secure-Diag	*OE.Enable-Disable-Secure-Diag*
OE.Secure-Diag-Usage	*OE.Secure-Diag-Usage*
OE.Composite-TOE-Id	*OE.Composite-TOE-Id*
OE.TOE-Id	*OE.TOE-Id*
	Additional objectives for the environment:
	OE.Secure-Values
	OE.Terminal-Support

6.2.2 Compatibility of Security Functional Requirements

258 All platform SFRs are relevant for this Composite ST.

259 The Composite ST SFRs do not show any conflict with the platform SFRs.

260 The following platform SFRs are used by this Composite ST because of their security properties providing protection against attacks to the TOE as a whole:

- FRU_FLT.2,
- FDP_SDC.1,
- FDP_SDI.2,
- FPT_PHP.3,
- FDP_ITT.1,
- FPT_ITT.1,
- FDP_IFC.1,

FPT_FLS.1 in order to generate a software reset,

FCS_RNG.1 for the provision of random numbers,

FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 for side-channel protection.

261 Complementary, the *Table 13* below shows the mapping between the Platform SFRs specifically used to implement a security service by SFRs of this Composite ST.

Table 13. Platform Security Functional Requirements vs. TOE Security Functional Requirements

Platform SFR	Composite ST SFRs
FRU_FLT.2	FRU_FLT.2

Table 13. Platform Security Functional Requirements vs. TOE Security Functional Requirements (continued)

Platform SFR	Composite ST SFRs
FPT_FLS.1	FPT_FLS.1
FMT_LIM.1 / Test	FMT_LIM.1 / Test
FMT_LIM.2 / Test	FMT_LIM.2 / Test
FAU_SAS.1	FAU_SAS.1
FDP_SDC.1	FDP_SDC.1
FDP_SDI.2	FDP_SDI.2
FPT_PHP.3	FPT_PHP.3
FDP_ITT.1	FDP_ITT.1
FPT_ITT.1	FPT_ITT.1
FDP_IFC.1	FDP_IFC.1
FCS_RNG.1 / PTG.2	FCS_RNG.1 / PTG.2
FCS_COP.1 / TDES	FCS_COP.1 / TDES FCS_COP.1 / MFPEV2-DES
FCS_COP.1 / AES	FCS_COP.1 / AES FCS_COP.1 / MFPEV2-AES
FDP_ACC.2 / Memories	FDP_ACC.2 / Memories
FDP_ACF.1 / Memories	FDP_ACF.1 / Memories
FMT_MSA.3 / Memories	FMT_MSA.3 / Memories
FMT_MSA.1 / Memories	FMT_MSA.1 / Memories
FMT_SMF.1 / Memories	FMT_SMF.1 / Memories
FIA_API.1	FIA_API.1
FMT_LIM.1 / Loader	FMT_LIM.1 / Loader
FMT_LIM.2 / Loader	FMT_LIM.2 / Loader
FTP_ITC.1 / Loader	FTP_ITC.1 / Loader
FDP_UCT.1 / Loader	FDP_UCT.1 / Loader
FDP_UIT.1 / Loader	FDP_UIT.1 / Loader
FDP_ACC.1 / Loader	FDP_ACC.1 / Loader
FDP_ACF.1 / Loader	FDP_ACF.1 / Loader
FMT_MSA.3 / Loader	FMT_MSA.3 / Loader
FMT_MSA.1 / Loader	FMT_MSA.1 / Loader
FMT_SMR.1 / Loader	FMT_SMR.1 / Loader
FIA_UID.1 / Loader	FIA_UID.1 / Loader

Table 13. Platform Security Functional Requirements vs. TOE Security Functional Requirements (continued)

Platform SFR	Composite ST SFRs
FIA_UAU.1 / Loader	FIA_UAU.1 / Loader
FMT_SMF.1 / Loader	FMT_SMF.1 / Loader
FPT_FLS.1 / Loader	FPT_FLS.1 / Loader
FAU_SAR.1 / Loader	FAU_SAR.1 / Loader
FAU_SAS.1 / Loader	FAU_SAS.1 / Loader
FTP_ITC.1 / Sdiag	FTP_ITC.1 / Sdiag
FAU_SAR.1 / Sdiag	FAU_SAR.1 / Sdiag
FMT_LIM.1 / Sdiag	FMT_LIM.1 / Sdiag
FMT_LIM.2 / Sdiag	FMT_LIM.2 / Sdiag

6.2.3 Compatibility of Security Assurance Requirements

262 The level of assurance of the TOE is EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.1, while the level of assurance of the Platform is EAL6 augmented with ALC_FLR.1.

263 Therefore, the set of Security Assurance Requirements of this composite evaluation is a subset of the Security Assurance Requirements of the underlying platform.

264 There is no conflict regarding the Security Assurance Requirements.

7 Identification

Table 14. TOE components

Platform identification				Library identification
IC Maskset name	IC version	Master identification number	Firmware version	MIFARE Plus EV2 version
K470B	B	0x0200	3.1.2	1.0.2

Table 15. Guidance documentation

Component description	Reference	Version
MIFARE Plus® EV2 library v1.0 for the ST31N platform devices - User manual	UM_ST31N_MFP_EV2	2
MIFARE Plus EV2 interface specification - Technical note	TN_MIFARE_Plus_EV2	3
MIFARE Plus® EV2 library 1.0.2 on ST31N platforms - Release note	RN_ST31N_MFP_EV2_1.0.2	2

Table 16. Sites list

Site	Address	Activities[1]
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	ES-DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	ES-DEV
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B 3d floor 1831 Diegem/Machelen Belgium	ES-DEV

[1] ES-DEV = development, IT = Network infrastructure

8 References

Table 17. Common Criteria

Component description	Reference	Version
Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017	CCMB-2017-04-001 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2017-04-002 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017	CCMB-2017-04-003 R5	3.1 Rev 5

Table 18. Platform Security Target

Ref	Component description	Reference	Version
[PF-ST]	ST31N600 A01 Security Target for composition	SMD_ST31N6000_ST_20_002	A01.3

Table 19. Protection Profile and other related standards

Ref	Component description	Reference	Version
[PP0084]	Eurosmart - Security IC Platform Protection Profile with Augmentation Packages	BSI-CC-PP-0084-2014	1.0
[AUG]	Smartcard Integrated Circuit Platform Augmentations, March 2002.		1.0
[JILSR]	Security requirements for post-delivery code loading, Joint Interpretation Library, February 2016		1.0

Table 20. Other standards

Ref	Identifier	Description
[1]	BSI-AIS20/AIS31	A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler BSI, Version 2.0, 18-09-2011
[2]	NIST SP 800-67	NIST SP 800-67 Rev.2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology
[3]	FIPS 197	FIPS 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 2001
[4]	NIST SP 800-38A	NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010

Table 20. Other standards

Ref	Identifier	Description
[5]	NIST SP 800-38B	NIST special publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), June 2016
[6]	ANSSI-PP0084.03	PP0084: Interpretations, ANSSI, April 2016

Appendix A Glossary

A.1 Terms

Authorised user

A user who may, in accordance with the TSP, perform an operation.

Composite product

Security IC product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation.

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

Electronic component(s) designed to perform processing and/or memory functions.

IC Dedicated Software

IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by ***ST***. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

IC Dedicated Test Software

That part of the IC Dedicated Software which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC developer

Institution (or its agent) responsible for the IC development.

IC manufacturer

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

IC packaging manufacturer

Institution (or its agent) responsible for the IC packaging and testing.

Initialisation data

Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC’s production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data)

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations.

Packaged IC

Security IC embedded in a physical package such as micromodules, DIPs, SOICs or TQFPs.

Pre-personalization data

Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases. If "Package 2: Loader dedicated for usage by authorized users only" is used the Pre-personalisation Data may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.

Secret

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security IC

Composition of the TOE, the Security IC Embedded Software, User Data, and the package.

Security IC Embedded SoftWare (ES)

Software embedded in the Security IC and not developed by the IC designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3.

Security IC embedded software (ES) developer

Institution (or its agent) responsible for the security IC embedded software development and the specification of IC pre-personalization requirements, if any.

Security attribute

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Sensitive information

Any information identified as a security relevant element of the TOE such as:

- the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
- the security IC embedded software,
- the IC dedicated software,
- the IC specification, design, development tools and technology.

Smartcard

A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

Subject

An entity within the TSC that causes operations to be performed.

Test features

All features and functions (implemented by the IC Dedicated Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

TOE Delivery

The period when the TOE is delivered which is after Phase 3 ***or Phase 1 in this Security target***.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data

All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

A.2 Abbreviations

Table 21. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI).
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1. R5.
CMAC	Cipher-based Message Authentication Code
DES	Data Encryption Standard.
EAL	Evaluation Assurance Level.
ES	Security IC Embedded Software.
ES-DEV	Embedded Software Development.
FIPS	Federal Information Processing Standard.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
MFPEV2	MIFARE Plus® EV2 1.0.2
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
ST	Context dependent : STMicroelectronics or Security Target.
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to *www.st.com/trademarks*. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.